

MULTIFUNKTIONALE DIGITALSYSTEME

Bedienungsanleitung für Wireless LAN

GN-1050



Sicherheitshinweise

■ Sicherheitshinweise für Benutzer

Dieses Produkt ist nach dem"Wireless Telegraphy Act" als"Drahtloses Equipment für Stationen mit geringer Sendeleistung" klassifiziert und erfordert keine Funklizenz. Das Gesetz verbietet jegliche Modifikation an diesem Produkt.

■ Über die TOSHIBA W-LAN Lösung

Dieses W-LAN Modul entspricht dem IEEE 802.11 Standard (Revision B/G). Das W-LAN Modul unterstützt Datenraten bis 54 Mbit/s.

- Das Modul ist von der Wi-Fi Alliance Wi-Fi (Wireless Fidelity) zertifiziert. Dies bedeutet, die W-LAN Hardware kommuniziert problemlos mit IEEE 802.11 B/G kompatiblen W-LAN Produkten anderer Hersteller.
- Voll kompatibel zu anderen W-LAN Systemen, die auf den Übertragungsverfahren Direct Sequence Spread Spectrum (DSSS)/Orthogonal Frequency Division Multiplexing (OFDM) beruhen und kompatibel mit dem IEEE 802.11 Standard (Revision B/G) sind.

❑ Wireless Interfunktionalität

TOSHIBA Wireless LAN Produkte arbeiten mit allen Wireless LAN Produkten zusammen, die auf den Übertragungsverfahren Direct Sequence Spread Spectrum (DSSS)/Orthogonal Frequency Division Multiplexing (OFDM) beruhen und entsprechen folgenden Standards:

- IEEE 802.11 Standard für Wireless LANs (Revision B/G).
- Wireless Fidelity (Wi-Fi) Zertifizierung.

❑ Wireless LAN und Auswirkungen auf die Gesundheit

Wireless LAN Produkte emittieren wie alle Sendegeräte elektromagnetische Strahlung. Der Energiegehalt ist bei Wireless LAN Geräten jedoch wesentlich geringer als bei anderen drahtlosen Kommunikationsgeräten wie z. B. Mobiltelefonen.
Da Wireless LAN Produkte allen bekannten Sicherheitsstandards und Empfehlungen entsprechen, ist TOSHIBA der Ansicht, dass der Betrieb derartiger Geräte für den Verbraucher sicher ist. Diese Standards und Empfehlungen spiegeln die übereinstimmende Meinung der wissenschaftlichen Gemeinschaft und entstanden nach Beratungen und Diskussionen wissenschaftlicher Ausschüsse unter Einbeziehung der neuesten Forschungsergebnisse.
In bestimmten Situationen kann der Betrieb von Wireless LAN jedoch vom verantwortlichen Personal bestimmter Organisationen eingeschränkt werden. Diese Situationen können sein:

- Verwendung von Wireless LAN Systemen an Bord eines Flugzeuges oder
- In anderen Umgebungen wo das Risiko von Funkstörungen/Interferenzen mit anderen Geräten besteht, und dies als kritisch eingestuft wird.

Falls Sie nicht sicher sind, ob Sie ein drahtloses Gerät in einer bestimmten Organisation oder Umgebung (z. B. Flughafengebäude) benutzen dürfen, fragen Sie bitte das zuständige Personal bevor Sie Wireless LAN Geräte einschalten.

❑ Sicherheitshinweise für kabellose Produkte

Bitte lesen Sie alle Sicherheitshinweise sorgfältig, bevor Sie unsere kabellosen Produkte verwenden.
Diese Anleitung enthält Sicherheitshinweise die Sie beachten sollten, um mögliche Gesundheitsschäden oder Geräteschäden zu vermeiden.

Haftungsbeschränkung

Für Schäden durch höhere Gewalt wie Erdbeben oder Bränden, die Einwirkung Dritter, Unfällen, beabsichtigte oder unbeabsichtigte Bedienungsfehler, nicht bestimmungsgemäßen Gebrauch oder Benutzung in nicht zugelassenen Umgebungen ist Toshiba nicht verantwortlich.
Für indirekte Schäden (Gewinneinbußen, Betriebsunterbrechungen, etc.) die durch die Produktverwendung oder mangelnder Produkteigenschaften entstehen können, ist Toshiba nicht verantwortlich.
Für Schäden, die durch die Nichtbeachtung der Hinweise in dieser Bedienungsanleitung entstehen, ist Toshiba nicht verantwortlich.
Für Schäden, die durch Fehlbedienung oder die gemeinsame Verwendung mit nicht von uns hergestellten Produkten entstehen, ist Toshiba nicht verantwortlich.

WARNUNG



Träger von Herzschrittmachern sollten mindestens 22 cm von diesem Produkt entfernt bleiben.
Radiowellen sind potentiell in der Lage, den Betrieb von Herzschrittmachern zu beeinträchtigen.
Verwenden Sie dieses Produkt nicht innerhalb von medizinischen Einrichtungen oder in der Nähe von medizinischen Geräten.
Funkwellen sind potentiell in der Lage, den Betrieb medizinischer Geräte zu beeinträchtigen und bei diesen Geräten Funktionsstörungen zu verursachen.
Benutzen Sie dieses Produkt ebenfalls nicht in der Nähe von automatisch gesteuerten Anlagen wie automatischen Türen oder Alarmanlagen.
Funkwellen sind potentiell in der Lage, den Betrieb dieser Geräte zu beeinträchtigen und Funktionsstörungen zu verursachen.
Prüfen Sie daher, ob beim Betrieb dieses Produkts an anderen Geräten Störungen durch Funkwellen auftreten. Benutzen Sie dieses Produkt nicht, wenn derartige Effekte auftreten.
Ansonsten könnten an diesen Geräten Fehlfunktionen oder Beschädigungen auftreten.

HINWEIS

Verwenden Sie das Produkt nicht in folgenden Umgebungen:
In unmittelbarer Näher zu Mikrowellenherden oder Geräten, die Magnetfelder, statische Elektrizität oder Funkwellen erzeugen.
Je nach Umgebungsbedingungen können Funkwellen so abgeschwächt werden, dass sie das Produkt nicht erreichen.
Bluetooth™ und Wireless LAN Geräte arbeiten im selben Frequenzbereich und können sich untereinander stören.
Falls Sie Bluetooth™ und Wireless LAN Geräte gleichzeitig nutzen, kann es vorkommen, dass Sie die optimale Netzwerkleistung nicht erreichen oder dass Sie die Netzwerkverbindung verlieren.

❑ Zulassungsinformationen

Das TOSHIBA Wireless LAN Modul muss entsprechend den Herstellerempfehlungen und der mitgelieferten Produktdokumentation installiert und verwendet werden. Dieses Gerät entspricht den folgenden Richtlinien und Sicherheitsstandards.

Die beschriebenen Standards gelten bei Betrieb mit der verfügbaren Antenne (GN-3010). Verwenden Sie für dieses Produkt keine anderen Antennen.

❑ Canada - Industry Canada (IC)

This device complies with RSS 210 of Industry Canada.
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.
L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes: (1) il ne doit pas produire de brouillage et (2) l'utilisateur du dispositif doit étre prét à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

❑ Europa - EU Zulassungserklärung CE 0984 ⓘ

Dieses Gerät erfüllt alle wesentlichen Anforderungen der Richtlinie 1999/5/EC entsprechend folgenden Standards:

EN 300 328:

Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM); Breitband-Übertragungssysteme; Datenübertragungseinrichtungen für das 2,4 GHz ISM Band mit Spreizspektrummodulation

EN 301 489-17:

Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM); Elektro-magnetische Verträglichkeit für Funkeinrichtungen und -dienste
Teil 17: Spezifische Bedingungen für 2,4 GHz Breitband-Datenübertragungssysteme und lokale 5 GHz Hochleistungs-Funknetze (RLAN Equipment)

EN 60950-1:

Sicherheit für informationstechnische Systeme inklusive elektrischer Bürosysteme

EN 50385:

Standard für Mobilfunk-Basisstationen und für schnurlose Telekommunikationsanlagen im Hinblick auf die Basisgrenz- und Referenzwerte bezüglich der Belastung von Personen gegenüber elektromagnetischen Feldern (110 MHz bis 40 GHz)

Hereby, TOSHIBA TEC, declares that this GN-1050 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
TOSHIBA TEC vakuuttaa täten että GN-1050 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Hierbij verklaart TOSHIBA TEC dat het toestel GN-1050 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Bij deze verklaart TOSHIBA TEC dat deze GN-1050 voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
Par la présente TOSHIBA TEC déclare que l'appareil GN-1050 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Par la présente, TOSHIBA TEC déclare que ce GN-1050 est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Härmed intygar TOSHIBA TEC att denna GN-1050 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Undertegnede TOSHIBA TEC erklarer herved, at følgende udstyr GN-1050 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Hiermit erklärt TOSHIBA TEC, dass sich dieser/diese/dieses GN-1050 in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)

Hiermit erklärt TOSHIBA TEC die Übereinstimmung des Gerätes GN-1050 mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TOSHIBA TEC ΔΗΛΩΝΕΙ ΟΤΙ GN-1050 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ
Η Toshiba TEC Corporation δηλώνει με το παρόν ότι το μοντέλο GN-1050 ασύρματου προσαρμογέα LAN συμμορφώνεται με τις βασικές απαιτήσεις και τις λοιπές σχετικές διατάξεις της Οδηγίας 1999/5/ΕΚ
Con la presente TOSHIBA TEC dichiara che questo GN-1050 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Por medio de la presente TOSHIBA TEC declara que el GN-1050 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
TOSHIBA TEC declara que este GN-1050 está conforme com os requisitos essenciais e outras disposicões da Directiva 1999/5/CE.
Toshiba TEC Corporation, GN-1050 model Kablosuz LAN Adaptörünün 1999/5/EC Tüzüğünün temel gereksinimlerine ve diğer ilgili uygulamalara uyduğunu beyan eder.
Thoshiba TEC Corpration timto prohlasuje, ze GN-1050 je ve shode se zakladnimi pozadavky a s dalsimi prislusnymi ustanoveni Narizeni vlady c. 426/2000 Sb.
Toshiba TEC Corporation declar prin prezenta c adaptorul fr fir LAN model GN-1050 este în conformitate cu cerinele eseniale i cu alte prevederi corespunztoare ale Directivei 1999/5/EC

❑ USA-Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by tuning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with part 15 of the FCC rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Labelling

Toshiba TEC Wireless LAN Module GN-1050 labelled as below.
FCC ID: BJI-GN1050
The proposed FCC ID label format is to be placed on the module. If FCC ID is not visible when the module is installed into the system, "Contains FCC ID:BJI-GN1050" shall be placed on the outside of final host system.

Caution: Exposure to Radio Frequency Radiation.
To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

❑ Regulatory Notice for Channel Use in France

The number of channels that can be used for wireless LAN differs from country to country. In France however, user only 4 channels (channel 10, 11, 12, 13) when using wireless networks.
- Channel 10 (2457 MHz)
- Channel 11 (2462 MHz)
- Channel 12 (2467 MHz)

- Channel 13 (2472 MHz)

France limited to 2446.5-2483.5 MHz Indoor use. Belgium limited to 2400-2483.5 MHz Indoor, 2460-2483.5 MHz Outdoor use.

❑ Landes- bzw. regionale Zulassungen für Toshiba Wireless LAN

Dieses Equipment hat eine Zulassung entsprechend den Funk- und Fernmeldegesetzen der jeweiligen Länder/Regionen. Für weiter Einzelheiten wenden Sie sich bitte an Ihren Toshiba-Vertriebspartner.

■ HINWEISE!

- Eine nicht genehmigte Reproduktion dieser Dokumentation, als Ganzes oder in Teilen, ist nicht gestattet.
- Spezifikationen, Form und Inhalt dieser Dokumentation können ohne vorherige Ankündigung geändert werden.
- Diese Dokumentation wurden mit größmöglicher Sorgfalt und Genauigkeit erstellt. Sollten Sie trotzdem Ungenauigkeiten oder Diskrepanzen feststellen, bitten wir Sie, dies einem unserer TOSHIBA-Vertriebspartner oder Servicetechniker mitzuteilen.
- Ungeachtet dessen ist es dem Hersteller nicht möglich, Ansprüche auf Verluste oder entgangenem Gewinn anzuerkennen, die durch die Verwendung dieses Produkts entstehen können.
- TOSHIBA TEC kann die vollständige Systemleistung nicht garantieren, wenn andere als die in dieser Anleitung beschriebenen Einstellungen vorgenommen werden.
- Microsoft, Windows, Windows NT sowie die Produktnamen anderer Microsoft-Produkte sind Handelsmarken der Microsoft Corporation in den USA und anderen Ländern.
  Andere genannte Firmen und Produktnamen sind Handelsmarken oder eingetragene Warenzeichen ihrer jeweiligen Eignetümer.
  Dieses Dokument enthält nicht die Symbole"™","®","©" etc.

INHALTSVERZEICHNIS



1

W-LAN EINRICHTEN

Dieser Abschnitt beschreibt Vorbereitungen für die W-LAN Einstellungen des Systems.

Vorbereitungen

Wir danken Ihnen für den Kauf des GN-1050 Wireless LAN Moduls.
Dieses Produkt verwendet ein 2,4 GHz Spreizspektrum-Übertragungssystem und ist mit dem IEEE Standard 802.11g und 802.11b kompatibel.

Bei aktiviertem W-LAN können folgende Druckverfahren verwendet werden:
- Raw TCP Druck von Windows Computern
- LPR Druck von Windows Computern
- LPR Druck von Macintosh Computern
- LPR Druck von Unix Workstations

Tipp

Die Einrichtung der Clientcomputer für den WiFi Druck ist identisch mit der für kabelgebundene Netzwerke. Einzelheiten hierzu siehe ***Druckanleitung***.

Hinweise

- Für den W-LAN Zugriff auf das System müssen die Clientcomputer ebenfalls über W-LAN Module verfügen.
- Wenn Sie W-LAN aktivieren, wird die interne NIC deaktiviert. W-LAN und kabelgebundenes LAN können nicht gleichzeitig verwendet werden.

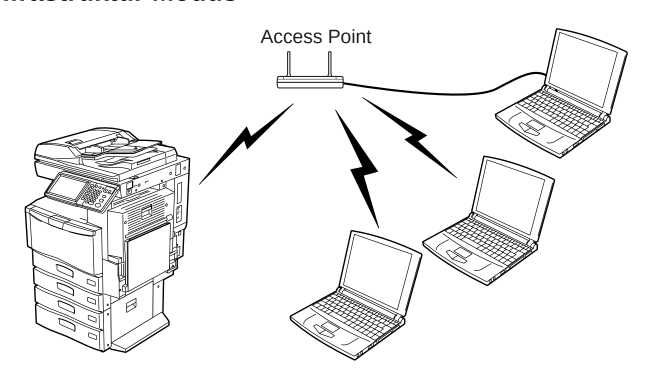
■ Installation vorbereiten

Bitte lesen Sie diesen Abschnitt, bevor Sie die W-LAN Einstellungen des Systems vornehmen.

❑ Netzwerktyp ermitteln

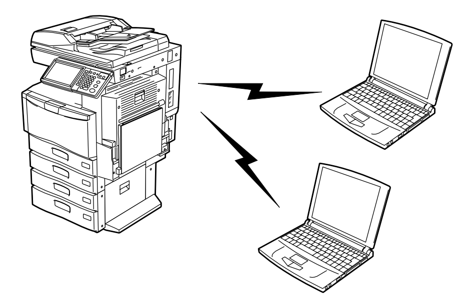
Dieses W-LAN Modul unterstützt die Modi Infrastruktur und Ad Hoc.

Infrastruktur Modus



Im Infrastruktur Modus erfolgt die Verbindungsaufnahme zum System über einen Access Point. Der Infrastruktur Modus ist für mehrere parallele Verbindungen gleichzeitig geeignet.
Der Infrastruktur Modus benötigt zwingend einen Access Point, über den die Netzwerkverbindungen geleitet werden.

Ad Hoc Modus



Im Ad Hoc Modus benötigt die Verbindungsaufnahme zum System keinen Access Point. Der Ad Hoc Modus ist nicht für mehrere parallele Verbindungen gleichzeitig geeignet, kann aber leichter konfiguriert werden, da der Access Point nicht erforderlich ist.

❑ SSID definieren

In einem W-LAN müssen alle Geräte die gleiche SSID (Service Set ID) besitzen. Nur Geräte mit gleicher SSID können über das W-LAN miteinander kommunizieren.

Im Infrastruktur Modus wird die SSID normalerweise im Access Point festgelegt. Daher muss für dieses System die gleiche SSID wie im Access Point eingestellt werden.

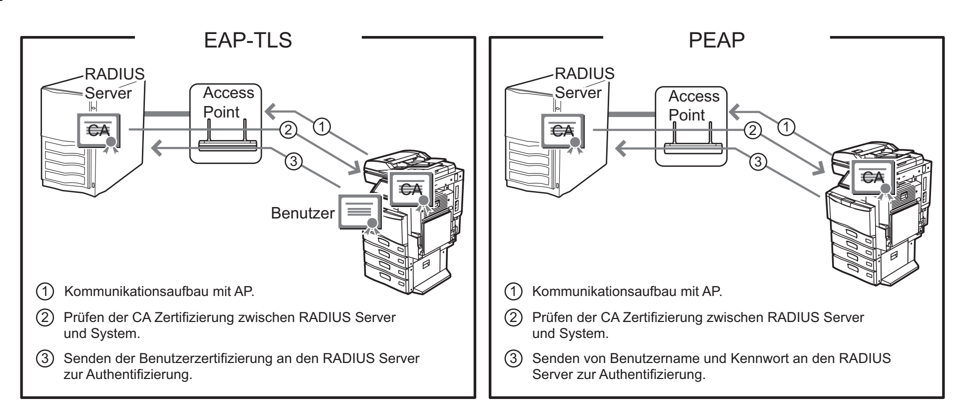
Im Ad Hoc Modus müssen Sie die gleiche SSID einstellen, die in den Clientcomputer eingestellt ist. Es können nur Geräte miteinander in Verbindung treten, denen die gleiche SSID zugewiesen wurde.

❑ Sicherheitsmodus definieren

Dieses Gerät unterstützt die folgenden Sicherheitsfunktionen.

WPA/WPA2

Mit WPA/WPA2 können Sie den Zugriff auf das W-LAN über einen RADIUS-Server kontrollieren. WPA/WPA2 ist nur im Infrastruktur Modus verfügbar.
Es existieren zwei Protokolle für WPA/WPA2, EAP-TLS oder PEAP.
Zur Verwendung der EAP-TLS Authentifizierung muss ein Anwenderzertifikat (DER, BASE64 oder PKCS#7 codiert) und ein CA-Zertifikat (privater Schlüssel PKCS#7 codiert) im System installiert werden. Das System verwendet das Anwenderzertifikat für die W-LAN Anmeldung und der RADIUS-Server identifiziert das System über Benutzer-ID und Kennwort.
Zur Verwendung von PEAP muss ein CA-Zertifikat (DER, BASE64 oder PKCS#7 codiert) im System installiert werden. Das System verwendet Benutzername und Kennwort für die W-LAN Anmeldung und der RADIUS-Server identifiziert das System über das CA-Zertifikat.



Hinweis

Dieses Gerät unterstützt folgende RADIUS-Server.
- Für EAP-TLS: Windows Server 2000, Windows Server 2003, Windows Server 2008, Funk Odyssey Server
- Für PEAP: Windows Server 2000, Windows Server 2003, Windows Server 2008

WPAPSK/WPA2PSK

WPAPSK/WPA2PSK ist eine Authentifizierungsmethode mit PSK (Pre-Shared Key) zwischen Access Point und weiteren Geräten. WPAPSK/WPA2PSK ist nur im Infrastruktur Modus verfügbar.
Zum Zugriff auf das W-LAN mit WPAPSK/WPA2PSK Authentifizierung, muss die gleiche PSK Path Phrase in Access Point und weiteren Geräten existieren. Wenn die PSKs zwischen Access Point und weiteren Geräten identisch sind, gibt der Access Point die Netzwerkverbindung frei.
WPAPSK/WPA2PSK verfügt aufgrund der besseren Datenverschlüsselung über eine höhere Sicherheitsstufe als WEP.
Dieses System unterstützt TKIP und AES(CCMP) Verschlüsselung für WPAPSK/WPA2PSK.
TKIP verwendet für die Pakete unterschiedliche Schlüssel, kombiniert mit einer Integritätsprüfung. Der Schlüssel wird in bestimmten, fest definierten, Intervallen geändert.
AES ist ein erweiterter kryptographischer Algorithmus der U.S. Regierung, der alternativ für DES und 3DES verwendet wird.
Diese Authentifizierungsmethoden sind geeignet für kleine WLANs, da hierbei im Gegensatz zur WPA/WPA2 Authentifizierung kein spezieller Server erforderlich ist.

Hinweis

Bei Verwendung von WPAPSK/WPA2PSK ist die Vergabe eines sicheren Kennworts empfehlenswert.

WEP

WEP ist eine Datenverschlüsselungsmethode mit WEP-Schlüssel zwischen Access Point und den anderen WLAN-Geräten. Im Vergleich zu WPA/WPA2 und WPAPSK/WPA2PSK ist WEP weniger sicher. Ist das WLAN im Infrastruktur-Modus konfiguriert und unterstützt der Access Point WPA/WPA2 oder WPAPSK/WPA2PSK, sollten die letztgenannten Methoden anstelle von WEP verwendet werden.
Die WEP-Authentifizierung ist sowohl für den Infrastruktur Modus und den Ad Hoc Modus verfügbar.

Infrastruktur Modus einrichten

Die W-LAN Einstellungen können über das Bedienfeld des Systems durchgeführt werden.
Führen Sie zur Einrichtung des Systems im Infrastruktur Modus die folgenden Schritte aus.

1. Netzwerktyp wählen
   S.15 “Netzwerktyp wählen”
2. SSID definieren
   S.18 “SSID definieren”
3. Sicherheitsmodus wählen
   S.21 “Sicherheitsmodus wählen”

■ Netzwerktyp wählen

Zunächst im ADMIN-Menü über den Touch-Screen die Position WIRELESS-EINSTELLUNG auswählen und danach den Netzwerktyp für das WLAN einstellen.



Wenn Sie nicht wissen, welchen Netzwerktyp Sie wählen sollen, lesen Sie folgenden Abschnitt.
S.12 “Netzwerktyp ermitteln”

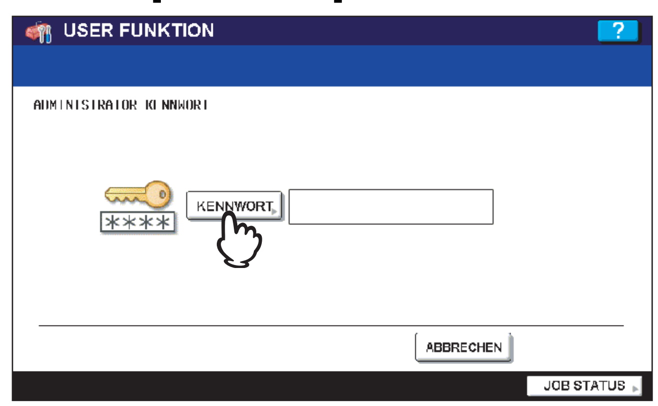
Netzwerktyp wählen

1 **Drücken Sie [USER FUNCTIONS] am Bedienfeld, um das Funktionsmenü aufzurufen.**

2 **Drücken Sie [ADMIN].**

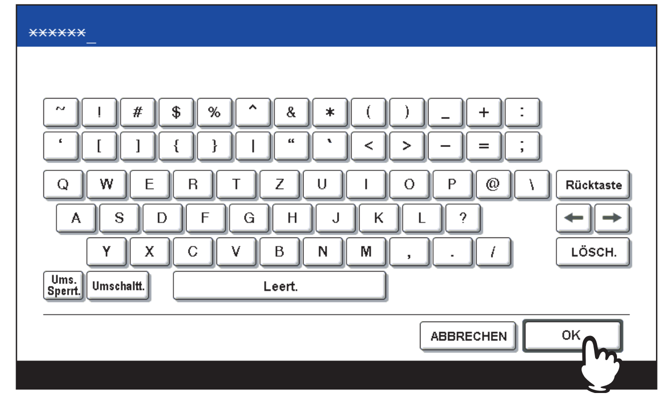
- Der Eingabebildschirm für das Administratorkennwort wird angezeigt.

3 **Drücken Sie [KENNWORT].**



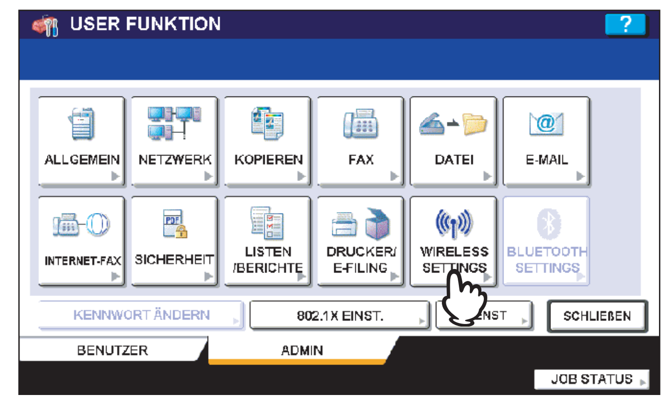
- Das Eingabefenster wird angezeigt.

4 **Geben Sie das Administratorkennwort ein und drücken Sie [OK].**



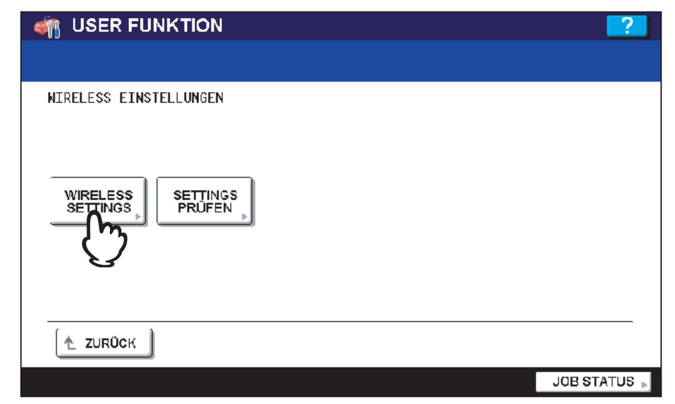
- Das ADMIN-Menü wird angezeigt.

5 Drücken Sie [WIRELESS SETTINGS].



- Das WLAN-Menü wird angezeigt.

6 Drücken Sie [WIRELESS SETTINGS].

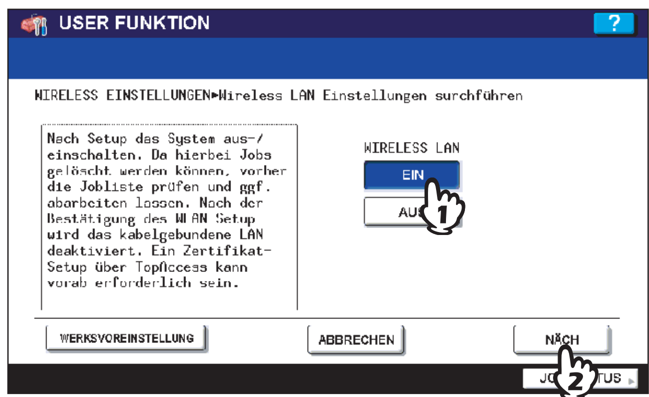


- Das Fenster WLAN-wird angezeigt.

Hinweis

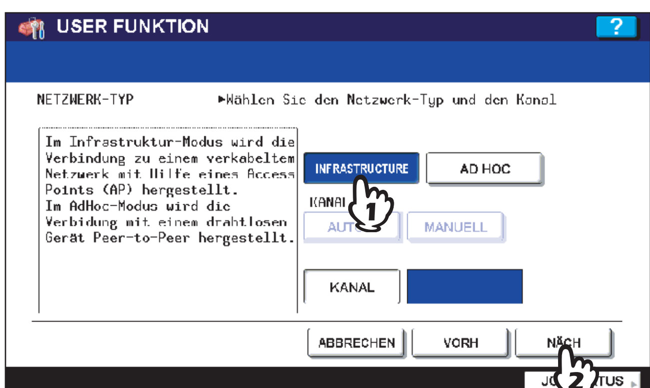
Die Anzeige kann sich etwas verzögern.

7 Drücken Sie [EIN] und [NÄCH].

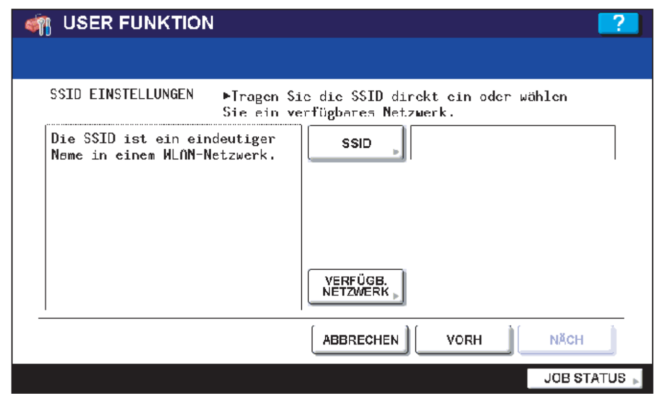


- Das Fenster NETZWERK TYP wird angezeigt.

8 Drücken Sie [INFRASTRUKTUR] und [NÄCH].



9 Das Fenster SSID wird angezeigt.



- Fahren Sie mit dem Definieren der SSID fort.
  S.18 “SSID definieren”

■ SSID definieren

Wenn als Netzwerktyp der Infrastruktur-Modus ausgewählt ist, können Sie die SSID über die Netzwerkliste auswählen oder die SSID manuell eingeben.
📖 S.18 “SSID aus Netzwerkliste auswählen”
📖 S.19 “SSID manuell eingeben”

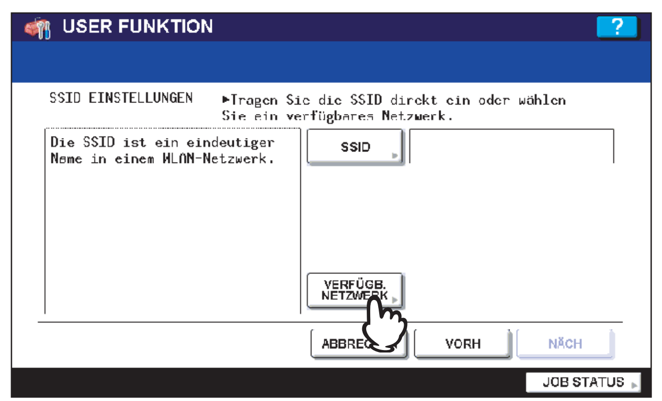


Wenn Sie nicht wissen, wie die SSID definiert werden muss, lesen Sie folgenden Abschnitt.
📖 S.13 “SSID definieren”

SSID aus Netzwerkliste auswählen

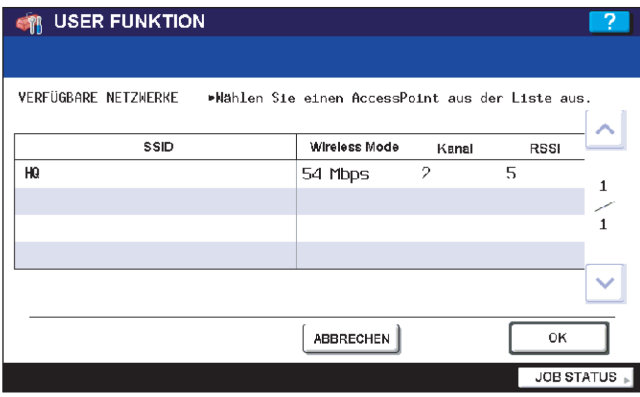
Das System kann die SSID automatisch aus dem W-LAN ermitteln. Danach können Sie die SSID aus der Liste auswählen.

1 Drücken Sie [VERFÜGB. NETZWERK].



- Das Fenster VERFÜGBARES NETZWERK wird angezeigt.

2 Wählen Sie die SSID mit der sich das System verbinden soll und drücken Sie [OK].

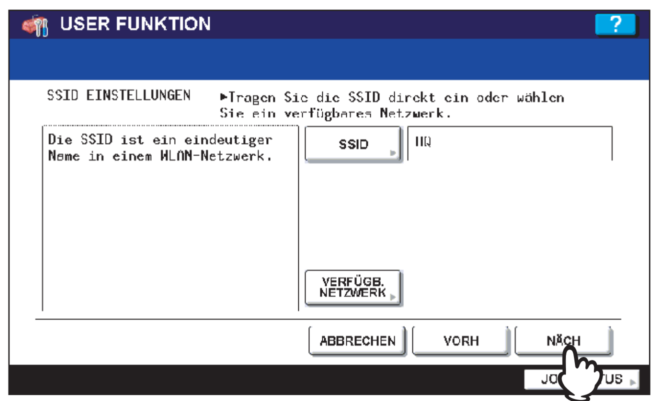


- Der Bildschirm SSID kehrt zurück.

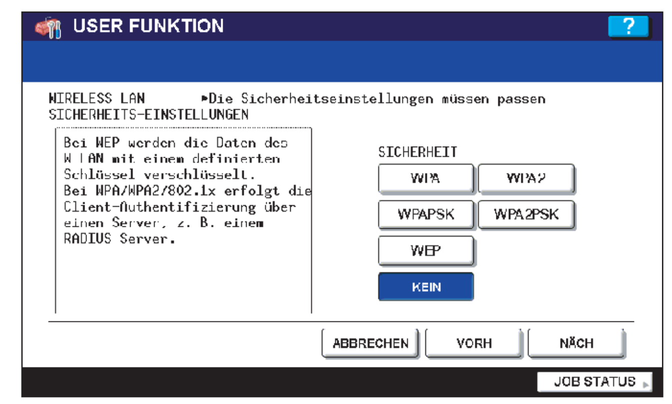
Hinweise

- Je nach Kommunikationsumgebung wird möglicherweise kein verfügbares Netzwerk angezeigt.
- Wenn die gewünschte SSID nicht erscheint, geben Sie sie manuell ein.
  📖 S.19 “SSID manuell eingeben”
- Dieses Wireless LAN unterstützt nur die Kanäle 1 bis 11. Wenn der Access Point andere Kanäle verwendet, kann das System nicht darauf zugreifen. Achten Sie daher darauf, dass die Kanäle 1 bis 11 im Access Point eingestellt sind.

3 **Drücken Sie [NÄCH].**



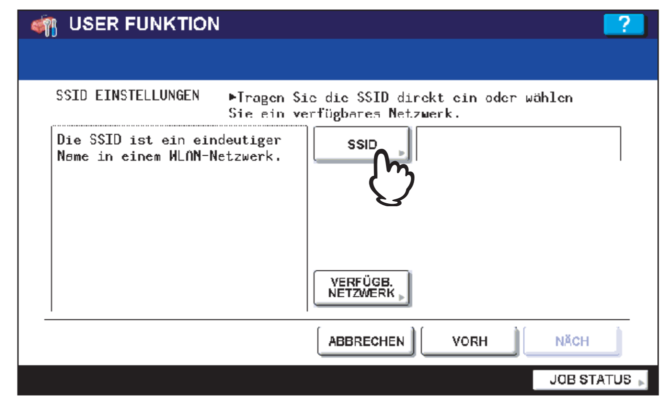
4 **Das Fenster WIRELESS-LAN SICHERHEITS-EINSTELLUNGEN wird angezeigt.**



- Fahren Sie mit dem Definieren des Sicherheitsmodus fort.
  S.21 “Sicherheitsmodus wählen”

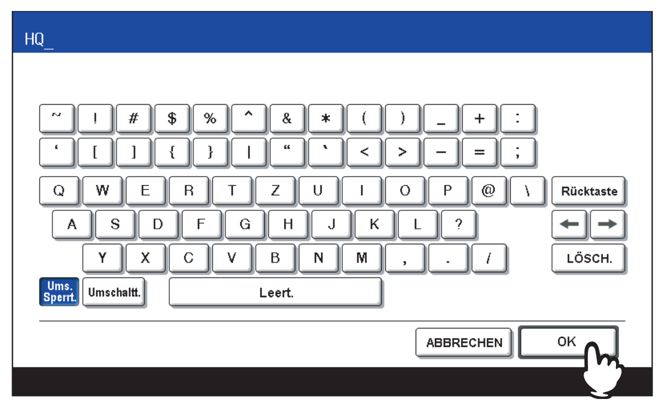
SSID manuell eingeben

1 **Drücken Sie [SSID].**



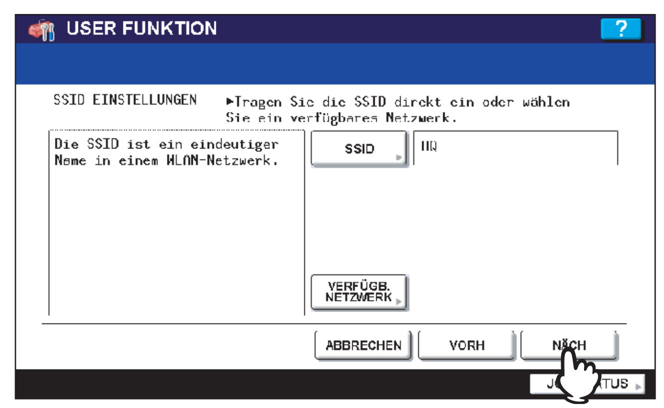
- Das Menü für die Buchstabeneingabe erscheint.

2 **Geben Sie die SSID mit der angezeigten Tastatur und den Zifferntasten ein und drücken Sie [OK].**

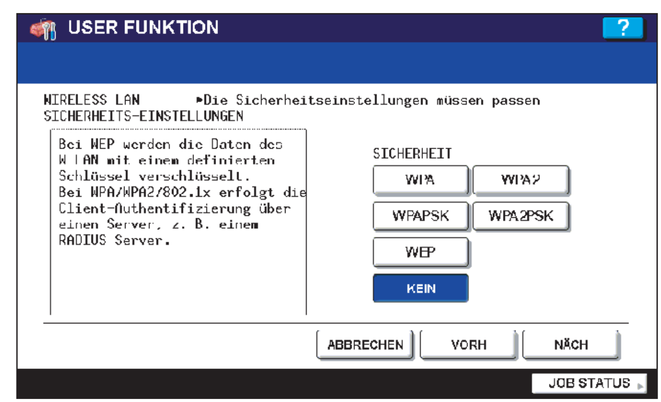


- Der Bildschirm SSID kehrt zurück.

3 **Drücken Sie [NÄCH].**



4 **Das Fenster WIRELESS-LAN SICHERHEITS-EINSTELLUNGEN wird angezeigt.**



- Fahren Sie mit dem Definieren des Sicherheitsmodus fort.
  📖 S.21 “Sicherheitsmodus wählen”

■ Sicherheitsmodus wählen

Wählen Sie nach der SSID einen geeigneten Sicherheitsmodus für Ihr W-LAN.
Die Vorgehensweise ist je nach Typ des Sicherheitsmodus unterschiedlich.

📖 S.21 “WPA/WPA2 mit EAP-TLS wählen”
📖 S.26 “WPA/WPA2 mit EAPP wählen”
📖 S.30 “WPAPSK/WPA2PSK wählen”
📖 S.32 “WEP auswählen”
📖 S.34 “Keinen Sicherheitsmodus wählen”

Hinweis

Wenn Sie nicht wissen, welchen des Sicherheitsmodus Sie wählen sollen, lesen Sie folgenden Abschnitt.
📖 S.13 “Sicherheitsmodus definieren”

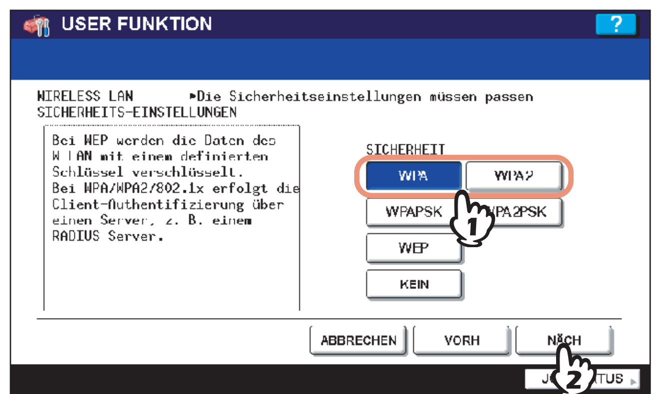
WPA/WPA2 mit EAP-TLS wählen

Für WPA/WPA2 mit EAP-TLS Protokoll müssen Sie ein Anwenderzertifikat und CA-Zertifikat im System installieren. Das System verwendet das Anwenderzertifikat für die W-LAN Anmeldung und der RADIUS-Server identifiziert das System über das CA-Zertifikat.

Hinweis

Für WPA/WPA2 mit EAP-TLS Protokoll müssen Sie Anwenderzertifikat und CA-Zertifikat mit TopAccess installieren. Einzelheiten hierzu siehe ***TopAccess-Anleitung***.

1 Drücken Sie [WPA] oder [WPA2] und [NÄCH].

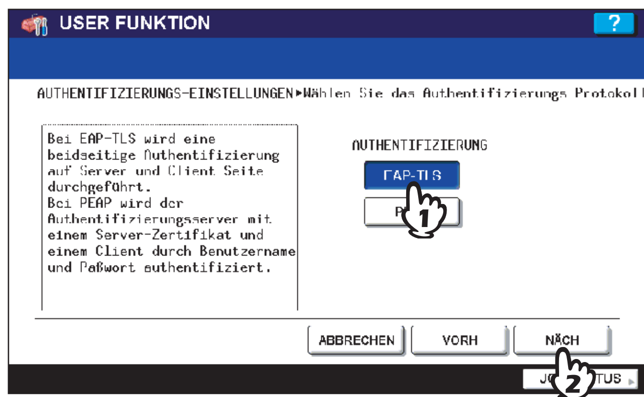


- Das Fenster AUTHENTIFIZIERUNG wird angezeigt.

Hinweis

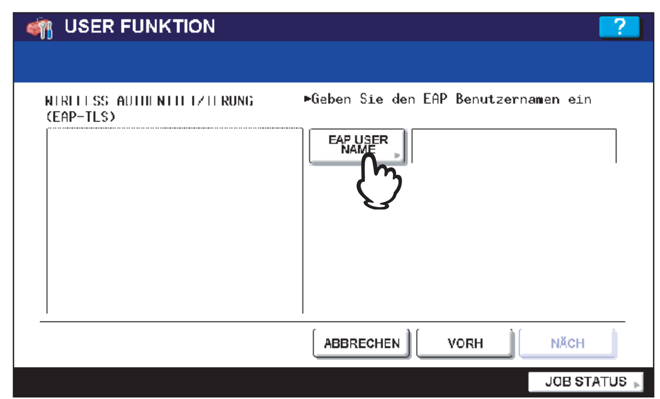
Wenn [WPA] oder [WPA2] ausgewählt ist, kann TKIP oder AES(CCMP) eingestellt werden.

2 Drücken Sie [EAP-TLS] und [NÄCH].



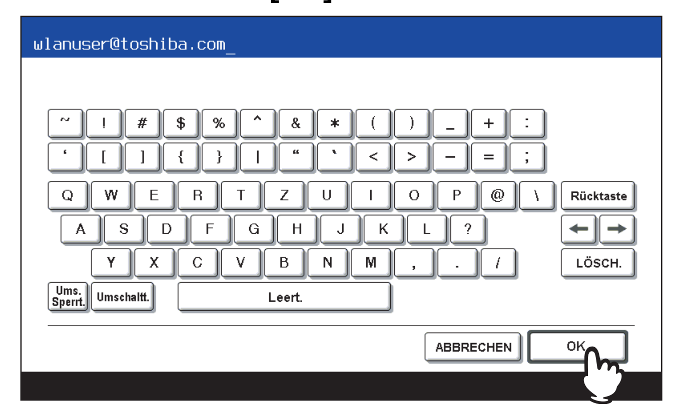
- Das Fenster AUTHENTIFIZIERUNG (EAP-TLS) wird angezeigt.

3 Drücken Sie [EAP USER NAME].



- Das Menü für die Buchstabeneingabe erscheint.

4 Geben Sie den EAP Benutzernamen mit der angezeigten Tastatur und den Zifferntasten ein und drücken Sie [OK].

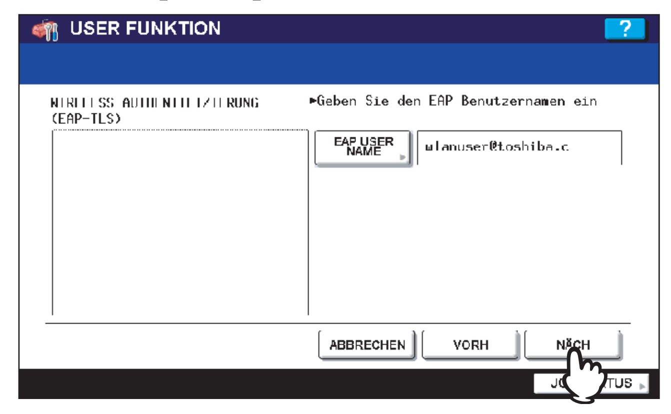


- Das Fenster AUTHENTIFIZIERUNG (EAP-TLS) kehrt zurück.

Hinweis

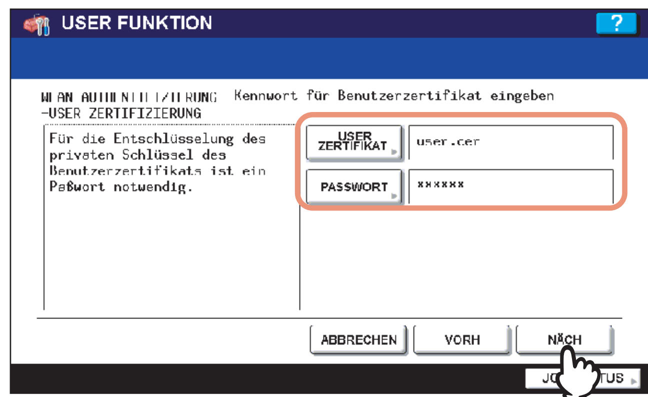
Geben Sie den Benutzernamen im Format “Benutzername@FQDN” ein.
Beispiel: wlanuser@toshiba.com

5 Drücken Sie [NÄCH].



- Das Fenster AUTHENTIFIZIERUNG - ANWENDERZERTIFIKAT wird angezeigt.

6 Definieren Sie folgende Positionen und drücken Sie [NÄCH].

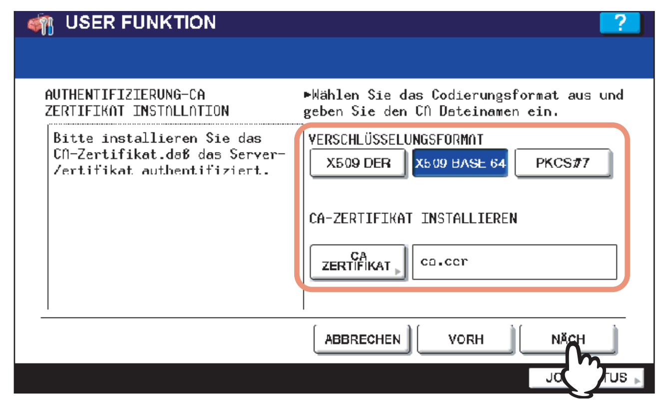


- **[ANWENDERZERTIFIKAT]**
  Drücken Sie darauf, um den Namen des Anwenderzertifikat einzugeben, das Sie mit TopAccess im System installiert haben. Ist die definierte Zertifikatdatei nicht im System installiert, wird eine Fehlermeldung angezeigt.
- **[KENNWORT]**
  Drücken Sie darauf, um das Kennwort für das Anwenderzertifikat einzugeben.

Tipp

Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

7 Definieren Sie folgende Positionen und drücken Sie [NÄCH].

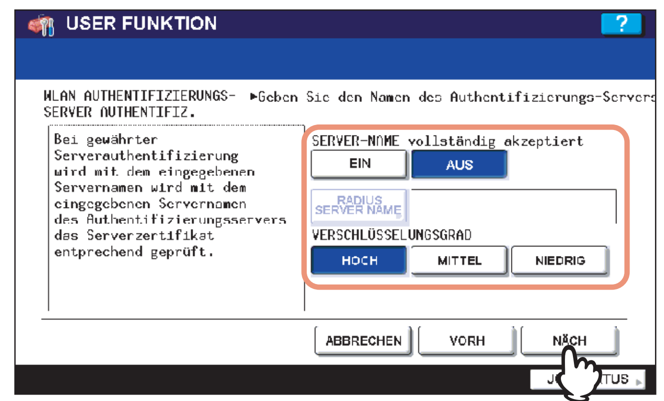


- **CODIERUNGSFORMAT**
  Wählen Sie das Codierungsformat für das CA-Zertifikat.
- **[CA-ZERTIFIKAT]**
  Drücken Sie darauf, um den Namen des CA-Zertifikats einzugeben, das Sie mit TopAccess im System installiert haben. Ist die definierte Zertifikatdatei nicht im System installiert, wird eine Fehlermeldung angezeigt.

Tipp

Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

8 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



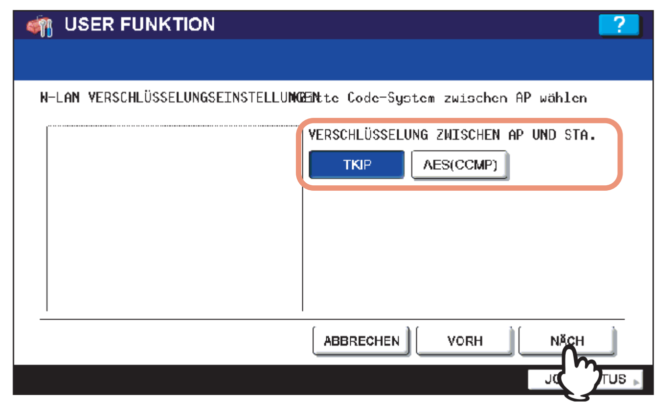
- **VOLLE ZUSTIMMUNG für SERVER NAME**
  Wählen Sie [EIN], um zu prüfen, ob der Name des RADIUS-Servers im Server-Zertifikat mit dem eingegeben Namen übereinstimmt. Wen n Sie [EIN] wählen, drücken Sie auf [RADIUS SERVER NAME], um den Namen einzugeben.

  Hinweis

  Geben Sie den RADIUS-Servernamen im Format “Servername@FQDN” ein.
  Beispiel: wlanserver@toshiba.com

- **VERSCHLÜSSELUNGSINTENSITÄT**
  Wählen Sie die Verschlüsselungsintensität.

9 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **VERSCHLÜSSELUNG ZWISCHEN AP UND STA.**
  Wählen Sie den Typ der Verschlüsselung für die Kommunikation zwischen Access Point und System.
  [TKIP] — Wählen Sie dies, wenn Sie TKIP verwenden wollen. TKIP verwendet für die Pakete unterschiedliche Schlüssel, kombiniert mit einer Integritätsprüfung. Der Schlüssel wird in bestimmten, fest definierten Intervallen geändert.
  [AES(CCMP)] — Wählen Sie dies, wenn Sie AES verwenden wollen. AES ist ein erweiterter kryptographischer Algorithmus der U.S. Regierung, der alternativ für DES und 3DES verwendet wird.

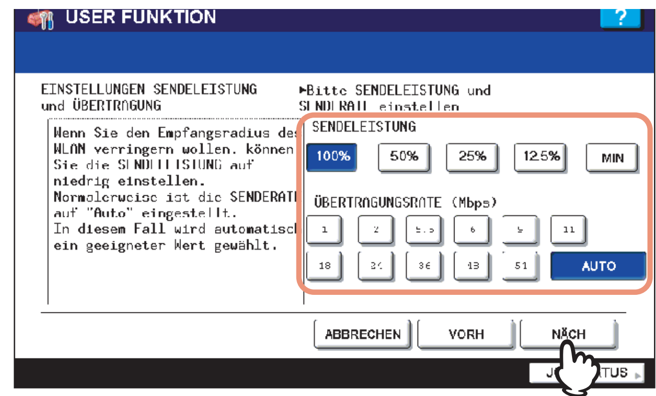
  Hinweis

  Wenn [WPA] oder [WPA2] ausgewählt ist, kann nur TKIP oder AES(CCMP) eingestellt werden.

  Tipp

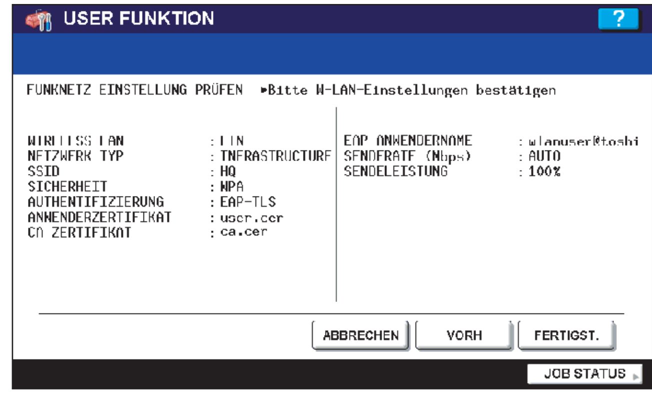
  Die Intensitätsreihenfolge ist:
  AES(CCMP) > TKIP

10 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **SENDELEISTUNG**
  Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].
- **SENDERATE**
  Wählen Sie die Senderate für die W-LAN Kommunikation. Wählen Sie [AUTO], wenn Sie die Senderate nicht begrenzen möchten. In der Einstellung[AUTO] passt das System die Senderate optimal an die gegebenen Bedingungen an.
  Im Allgemeinen wird [AUTO] gewählt. Nur wenn Kommunikationsprobleme auftreten, sollten Sie versuchsweise eine feste Rate einstellen.

11 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

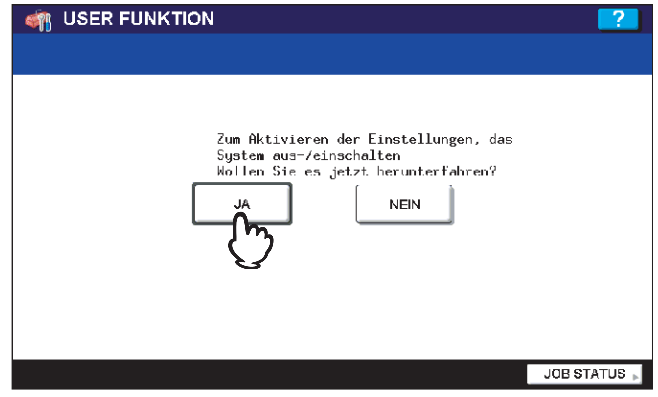


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

12 Drücken Sie [JA], um das System herunter zu fahren.



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

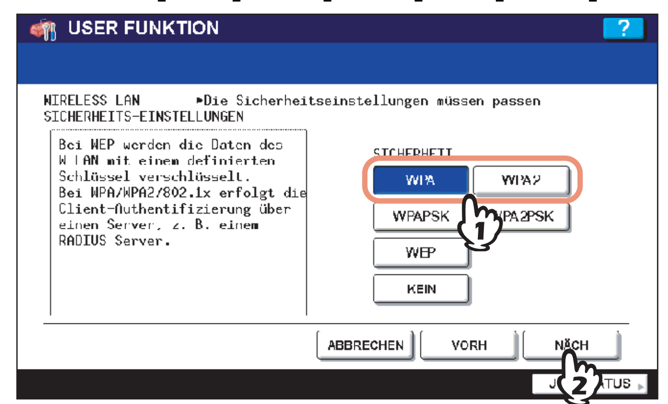
WPA/WPA2 mit EAPP wählen

Für WPA/WPA2 mit PEAP Protokoll müssen Sie ein CA-Zertifikat im System installieren. Das System verwendet Benutzername und Kennwort für die W-LAN Anmeldung und der RADIUS-Server identifiziert das System über das CA-Zertifikat.

Hinweis

Für WPA/WPA2 mit PEAP Protokoll müssen Sie mit TopAccess ein CA-Zertifikat im System installieren. Einzelheiten hierzu siehe ***TopAccess-Anleitung***.

1 Drücken Sie [WPA] oder [WPA2] und [NÄCH].

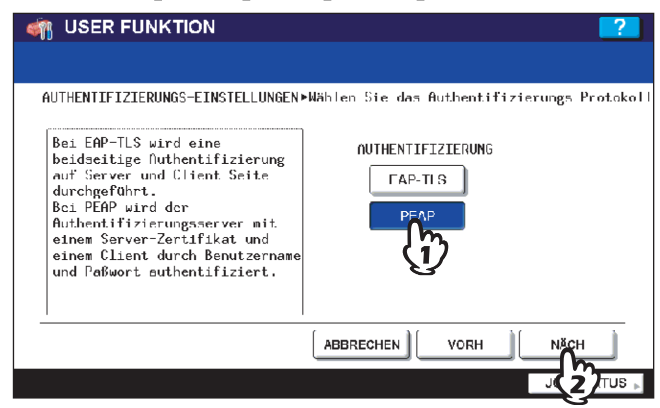


- Das Fenster AUTHENTIFIZIERUNG wird angezeigt.

Hinweis

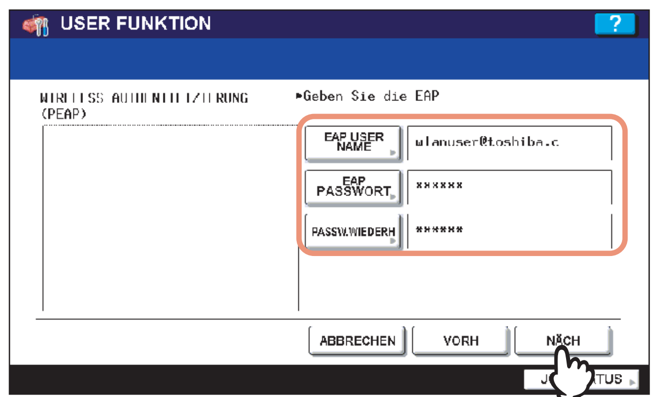
Wenn [WPA] oder [WPA2] ausgewählt ist, kann TKIP oder AES(CCMP) eingestellt werden.

2 Drücken Sie [PEAP] und [NÄCH].



- Das Fenster AUTHENTIFIZIERUNG (EAP-TLS) wird angezeigt.

3 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **[EAP BENUTZERNAME]**
  Drücken Sie darauf, um einen EAP-Benutzernamen einzugeben, der für die Anmeldung verwendet werden soll.



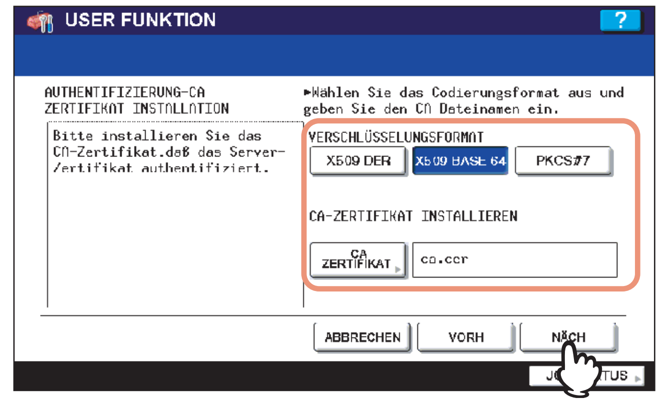
Geben Sie den Benutzernamen im Format “Benutzername@FQDN” ein.
Beispiel: wlanuser@toshiba.com

- **[EAP KENNWORT]**
  Drücken Sie darauf, um ein EAP-Kennwort einzugeben, das für die Anmeldung verwendet werden soll.
- **[KENNWORT WIEDERHOLEN]**
  Drücken Sie darauf, um das EAP-Kennwort erneut einzugeben.

Tipp

Wenn Sie auf die verschiedenen Tasten tippen, wird das Eingabefenster angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

4 Definieren Sie folgende Positionen und drücken Sie [NÄCH].

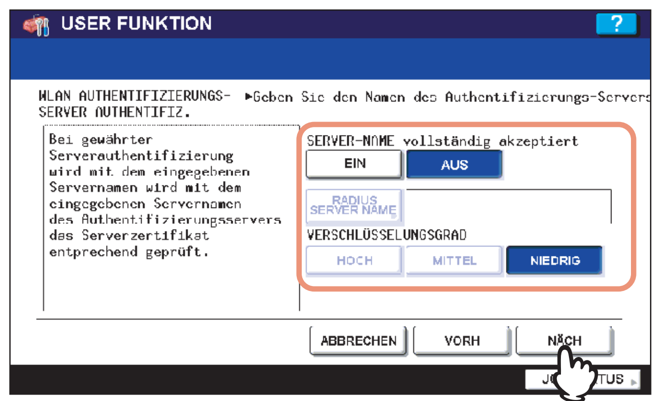


- **CODIERUNGSFORMAT**
  Wählen Sie das Codierungsformat für das CA-Zertifikat.
- **[CA-ZERTIFIKAT]**
  Drücken Sie darauf, um den Namen des CA-Zertifikats einzugeben, das Sie mit TopAccess im System installiert haben. Ist die definierte Zertifikatdatei nicht im System installiert, wird eine Fehlermeldung angezeigt.

Tipp

Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

5 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



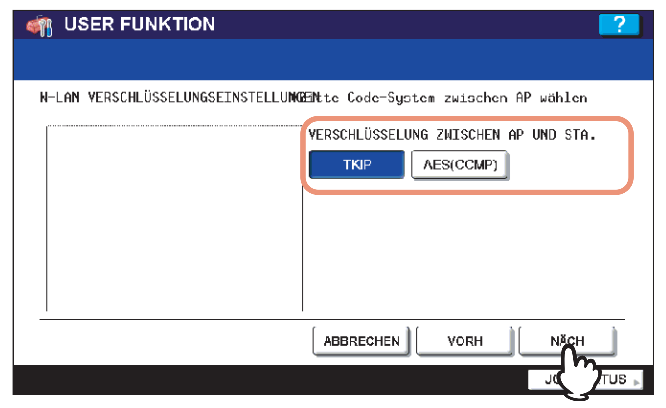
- **VOLLE ZUSTIMMUNG für SERVER NAME**
  Wählen Sie [EIN], um zu prüfen, ob der Name des RADIUS-Servers im Server-Zertifikat mit dem eingegeben Namen übereinstimmt. Wenn Sie [EIN] wählen, drücken Sie auf [RADIUS SERVER NAME], um den Namen einzugeben.

  Hinweis

  Geben Sie den RADIUS-Servernamen im Format “Servername@FQDN” ein.
  Beispiel: wlanserver@toshiba.com

- **VERSCHLÜSSELUNGSINTENSITÄT**
  Wählen Sie die Verschlüsselungsintensität. Für das PEAP-Protokoll kann nur [GERING] ausgewählt werden.

6 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **VERSCHLÜSSELUNG ZWISCHEN AP UND STA.**
  Wählen Sie den Typ der Verschlüsselung für die Kommunikation zwischen Access Point und System.
  [TKIP] — Wählen Sie dies, wenn Sie TKIP verwenden wollen. TKIP verwendet für die Pakete unterschiedliche Schlüssel, kombiniert mit einer Integritätsprüfung. Der Schlüssel wird in bestimmten, fest definierten Intervallen geändert.
  [AES(CCMP)] — Wählen Sie dies, wenn Sie AES verwenden wollen. AES ist ein erweiterter kryptographischer Algorithmus der U.S. Regierung, der alternativ für DES und 3DES verwendet wird.

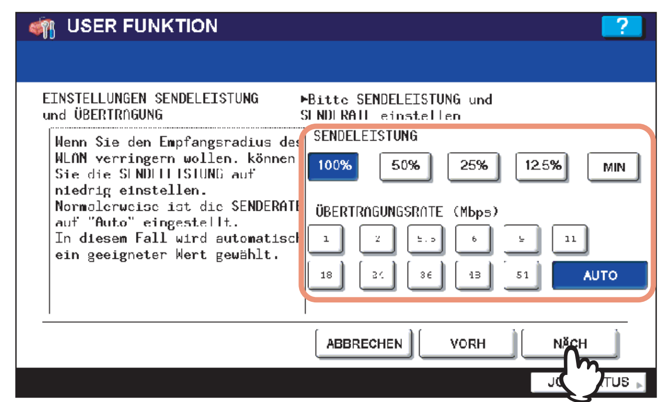
  Hinweis

  Wenn [WPA] oder [WPA2] ausgewählt ist, kann nur TKIP oder AES(CCMP) eingestellt werden.

  Tipp

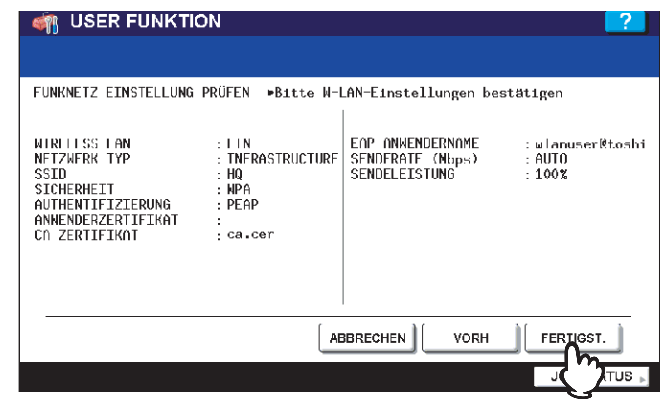
  Die Intensitätsreihenfolge ist:
  AES(CCMP) > TKIP

7 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **SENDELEISTUNG**
  Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].
- **SENDERATE**
  Wählen Sie die Senderate für die W-LAN Kommunikation. Wählen Sie [AUTO], wenn Sie die Senderate nicht begrenzen möchten. In der Einstellung [AUTO] passt das System die Senderate optimal an die gegebenen Bedingungen an.
  Im Allgemeinen wird [AUTO] gewählt. Nur wenn Kommunikationsprobleme auftreten, sollten Sie versuchsweise eine feste Rate einstellen.

8 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

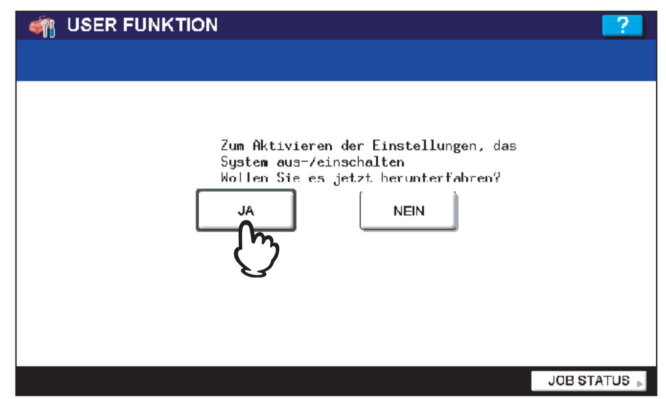


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

9 Drücken Sie [JA], um das System herunter zu fahren.

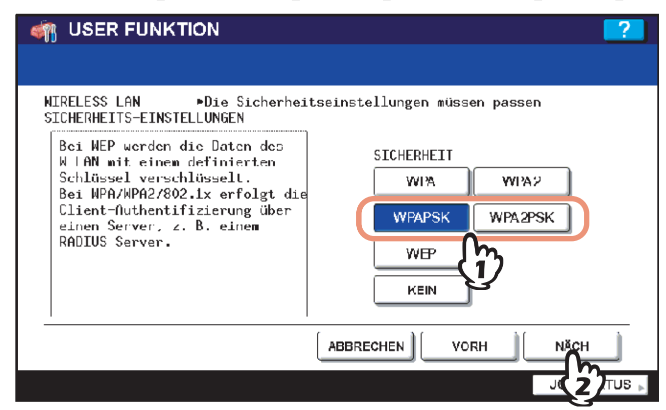


- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

WPAPSK/WPA2PSK wählen

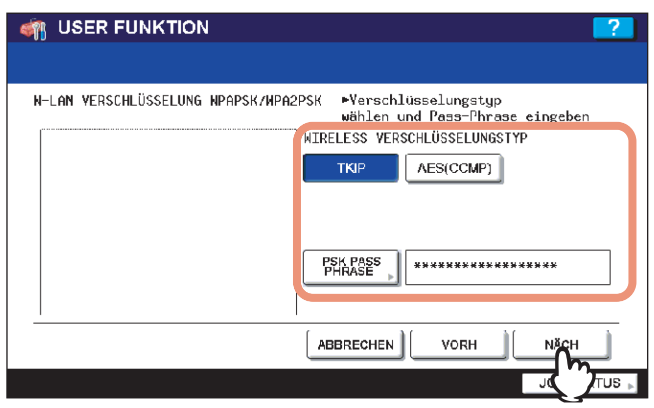
WPAPSK/WPA2PSK ist eine Authentifizierungsmethode mit PSK (Pre-Shared Key) zwischen Access Point und weiteren Geräten.
Zum Zugriff auf das W-LAN mit WPAPSK/WPA2PSK Authentifizierung, muss die gleiche PSK Path Phrase in Access Point und weiteren Geräten existieren. Wenn die PSKs zwischen Access Point und weiteren Geräten identisch sind, gibt der Access Point die Netzwerkverbindung frei.

1 Drücken Sie [WPAPSK] oder [WPA2PSK] und [NÄCH].



- Das Fenster VERSCHLÜSSELUNG WPA-PSK wird angezeigt.

2 Definieren Sie folgende Positionen und drücken Sie [NÄCH].

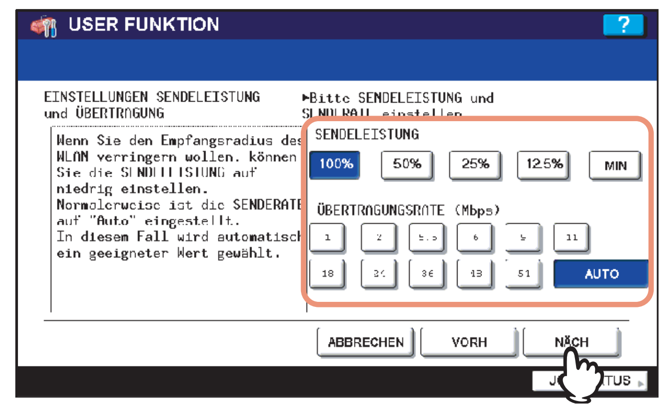


- **WLAN VERSCHLÜSSELUNGSTYP**
  Wählen Sie den Verschlüsselungstyp für PSK.
  [TKIP] — Wählen Sie dies, wenn Sie TKIP verwenden wollen. TKIP verwendet für die Pakete unterschiedliche Schlüssel, kombiniert mit einer Integritätsprüfung. Der Schlüssel wird in bestimmten, fest definierten Intervallen geändert.
  [AES(CCMP)] — Wählen Sie dies, wenn Sie AES verwenden wollen. AES ist ein erweiterter kryptographischer Algorithmus der U.S. Regierung, der alternativ für DES und 3DES verwendet wird.
- **[PSK PASS PHRASE]**
  Drücken Sie dies, um die PSK Pass Phrase einzugeben. PSK wird über die Pass Phrase erzeugt. Sie müssen die gleiche Pass Phrase eingeben, die im Access Point eingestellt ist. Die Länge der PSK Pass Phrase kann zwischen 8 bis 63 Zeichen betragen.

Tipp

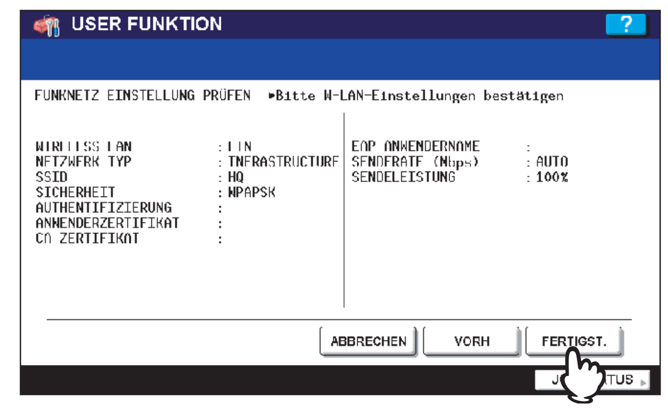
Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

3 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **SENDELEISTUNG**
  Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].
- **SENDERATE**
  Wählen Sie die Senderate für die W-LAN Kommunikation. Wählen Sie [AUTO], wenn Sie die Senderate nicht begrenzen möchten. In der Einstellung [AUTO] passt das System die Senderate optimal an die gegebenen Bedingungen an.
  Im Allgemeinen wird [AUTO] gewählt. Nur wenn Kommunikationsprobleme auftreten, sollten Sie versuchsweise eine feste Rate einstellen.

4 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

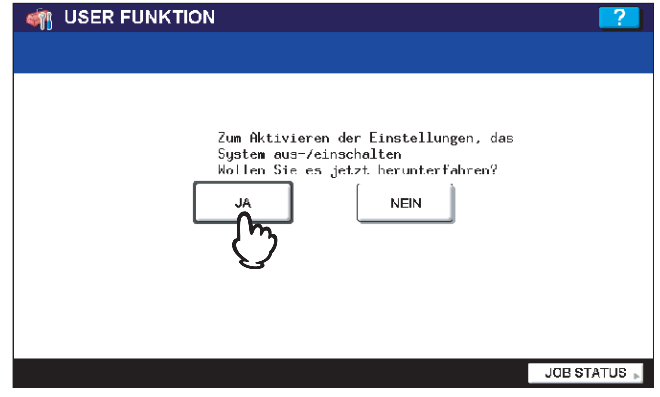


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

5 Drücken Sie [JA], um das System herunter zu fahren.

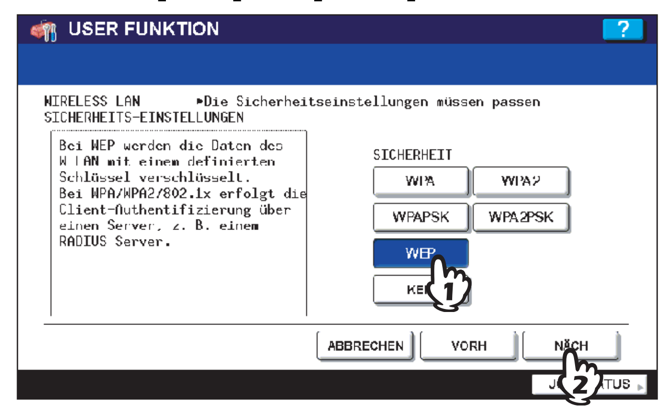


- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

WEP auswählen

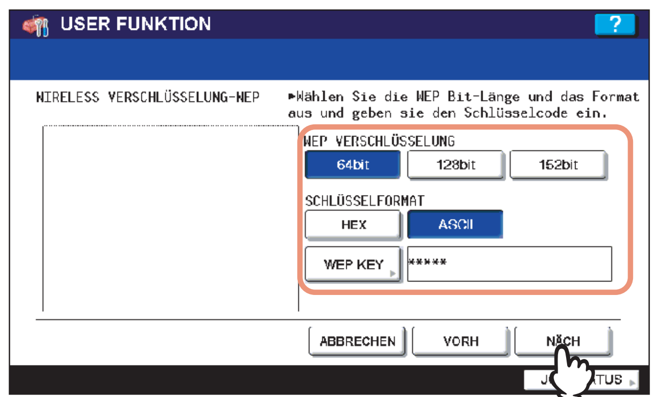
WEP ist eine Datenverschlüsselungsmethode mit WEP-Schlüssel zwischen Access Point und den anderen WLAN-Geräten. Im Vergleich zu WPA/WPA2 und WPAPSK/WPA2PSK ist WEP weniger sicher. Ist das WLAN im Infrastruktur-Modus konfiguriert und unterstützt der Access Point WPA/WPA2 oder WPAPSK/WPA2PSK, sollten die letztgenannten Methoden anstelle von WEP verwendet werden.

1 Drücken Sie [WEP] und [NÄCH].



- Das Fenster VERSCHLÜSSELUNG - WEP wird angezeigt.

2 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



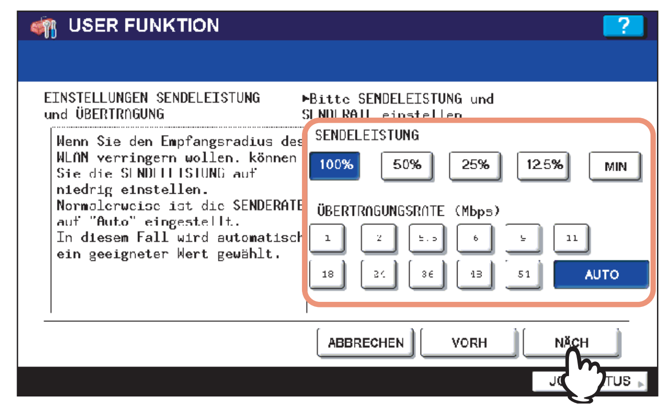
- **WEP VERSCHLÜSSELUNG**
  Wählen Sie die Bit-Länge des WEP-Schlüssels.
- **EINGABEMETHODE SCHLÜSSEL**
  Wählen Sie den Zeichencode des WEP-Schlüssels.
- **[WEP SCHLÜSSEL]**
  Drücken Sie darauf, um den WEP-Schlüssel einzugeben.
  Die maximale Länge des WEP-Schlüssels ist abhängig von der WEP-Verschlüsselung und der Schlüssel-Eingabemethode.

	64bit	128bit	152bit
HEX :	10	26	32
ASCII :	5	13	16


Tipp

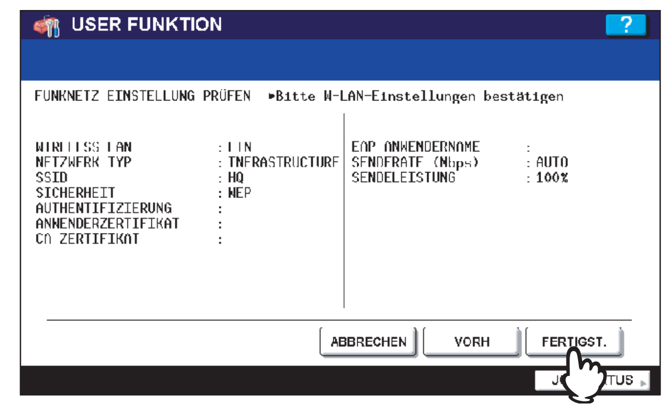
Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

3 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **SENDELEISTUNG**
  Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].
- **SENDERATE**
  Wählen Sie die Senderate für die W-LAN Kommunikation. Wählen Sie [AUTO], wenn Sie die Senderate nicht begrenzen möchten. In der Einstellung [AUTO] passt das System die Senderate optimal an die gegebenen Bedingungen an.
  Im Allgemeinen wird [AUTO] gewählt. Nur wenn Kommunikationsprobleme auftreten, sollten Sie versuchsweise eine feste Rate einstellen.

4 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

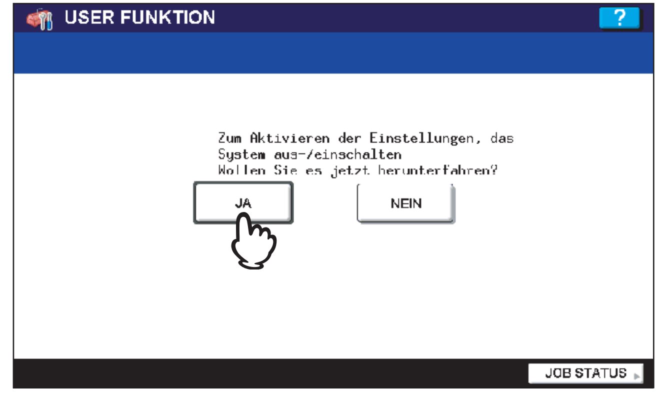


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

5 Drücken Sie [JA], um das System herunter zu fahren.



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

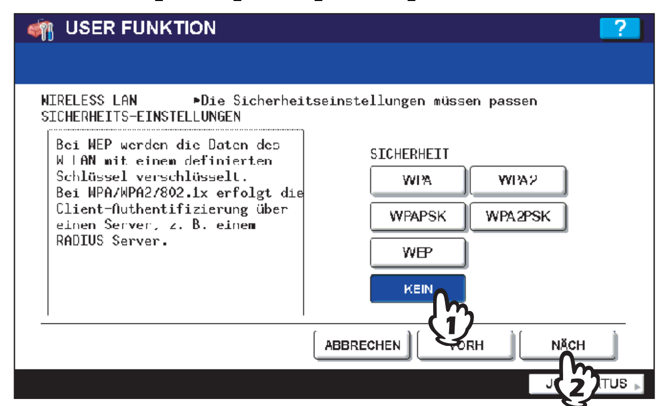
Keinen Sicherheitsmodus wählen

Sie können das W-LAN auch ungesichert betreiben.

Hinweis

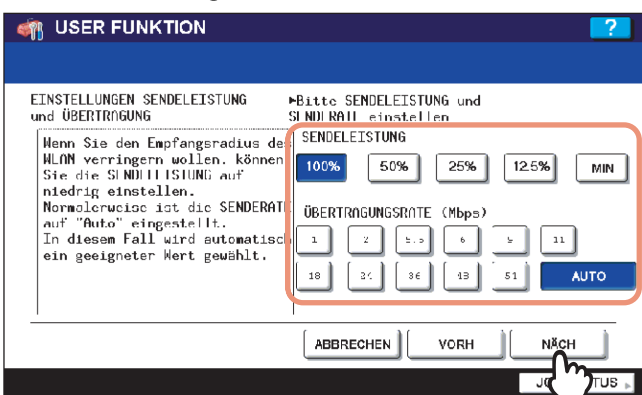
Wenn Sie dies einstellen, kann sich jeder, der die SSID in Erfahrung bringt, mit dem W-LAN verbinden. Wir empfehlen daher dringend einen Sicherheitsmodus einzustellen.

1 Drücken Sie [KEIN] und [NÄCH].



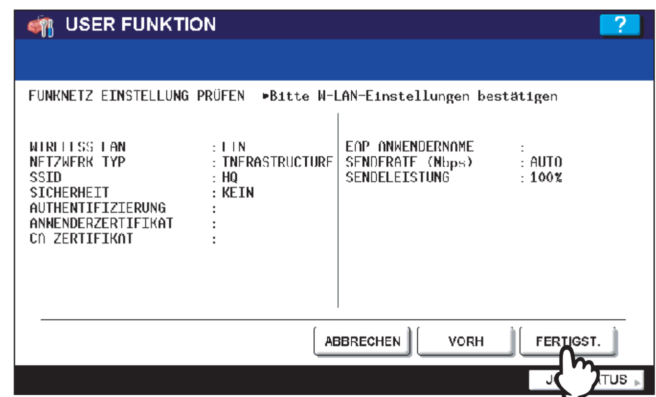
- Die Fenster SENDELEISTUNG und SENDERATE werden angezeigt.

2 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **SENDELEISTUNG**
  Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].
- **SENDERATE**
  Wählen Sie die Senderate für die W-LAN Kommunikation. Wählen Sie [AUTO], wenn Sie die Senderate nicht begrenzen möchten. In der Einstellung [AUTO] passt das System die Senderate optimal an die gegebenen Bedingungen an.
  Im Allgemeinen wird [AUTO] gewählt. Nur wenn Kommunikationsprobleme auftreten, sollten Sie versuchsweise eine feste Rate einstellen.

3 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

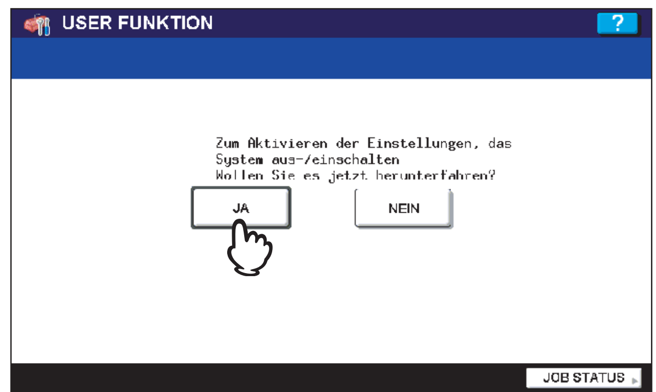


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

4 Drücken Sie [JA], um das System herunter zu fahren.



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

Ad Hoc Modus einrichten

Die W-LAN Einstellungen können über das Bedienfeld des Systems durchgeführt werden.
Führen Sie zur Einrichtung des Systems im Infrastruktur Modus die folgenden Schritte aus.

1. Netzwerktyp wählen
   📖 S.36 “Netzwerktyp wählen”
2. SSID definieren
   📖 S.39 “SSID definieren”
3. Sicherheitsmodus wählen
   📖 S.41 “Sicherheitsmodus wählen”

■ Netzwerktyp wählen

Zunächst im ADMIN-Menü über den Touch-Screen die Position WIRELESS-EINSTELLUNG auswählen und danach den Netzwerktyp für das WLAN einstellen.



Wenn Sie nicht wissen, welchen Netzwerktyp Sie wählen sollen, lesen Sie folgenden Abschnitt.
📖 S.12 “Netzwerktyp ermitteln”

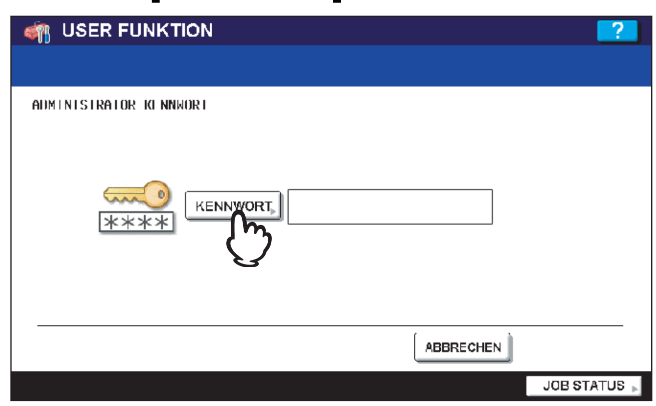
Netzwerktyp wählen

1 **Drücken Sie [USER FUNCTIONS] am Bedienfeld, um das Funktionsmenü aufzurufen.**

2 **Drücken Sie [ADMIN].**

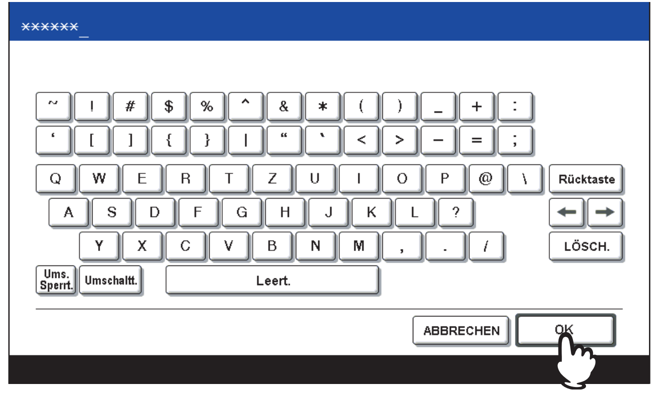
- Der Eingabebildschirm für das Administratorkennwort wird angezeigt.

3 **Drücken Sie [KENNWORT].**



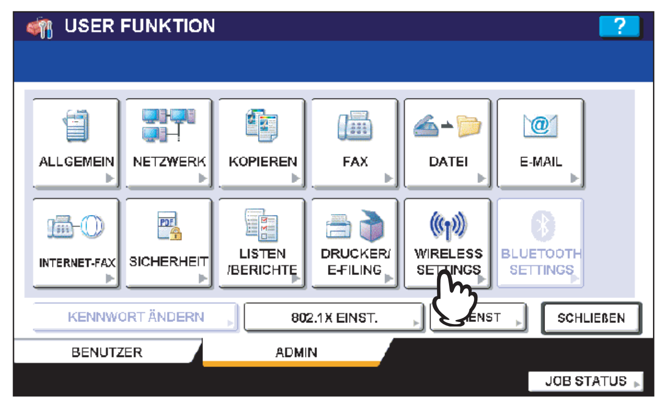
- Das Eingabefenster wird angezeigt.

4 **Geben Sie das Administratorkennwort ein und drücken Sie [OK].**



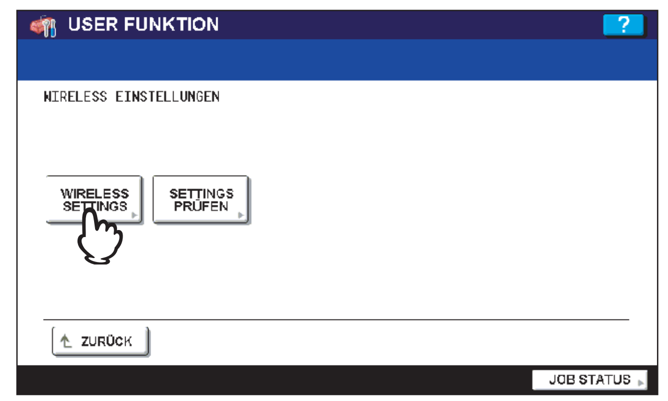
- Das ADMIN-Menü wird angezeigt.

5 Drücken Sie [WIRELESS SETTINGS].



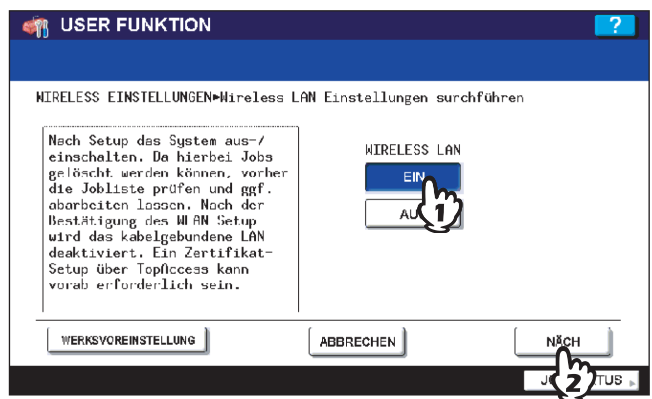
- Das WLAN-Menü wird angezeigt.

6 Drücken Sie [WIRELESS SETTINGS].



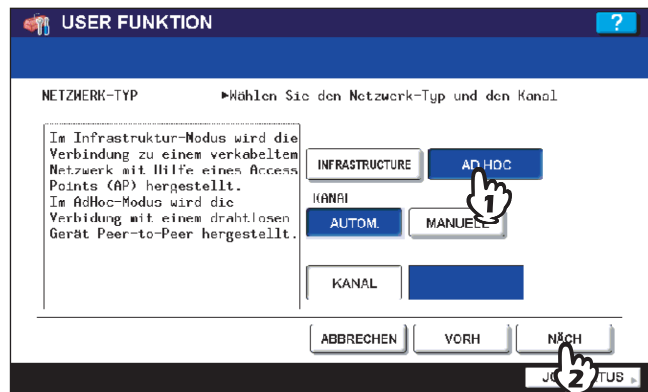
- Das Fenster WLAN wird angezeigt.

7 Drücken Sie [EIN] und [NÄCH].



- Das Fenster NETZWERK TYP wird angezeigt.

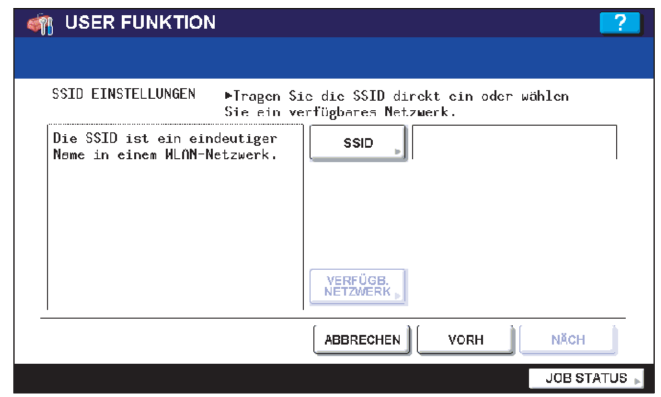
8 Drücken Sie [AD HOC] und [NÄCH].



Hinweis

Sie können die Kanäle von 1 bis 11 wählen. Falls schon ein Kanal für das Ad Hoc Netzwerk verwendet wird, sollten Sie diesen wählen.

9 Das Fenster SSID wird angezeigt.



- Fahren Sie mit dem Definieren der SSID fort.
  📖 S.18 “SSID definieren”

■ SSID definieren

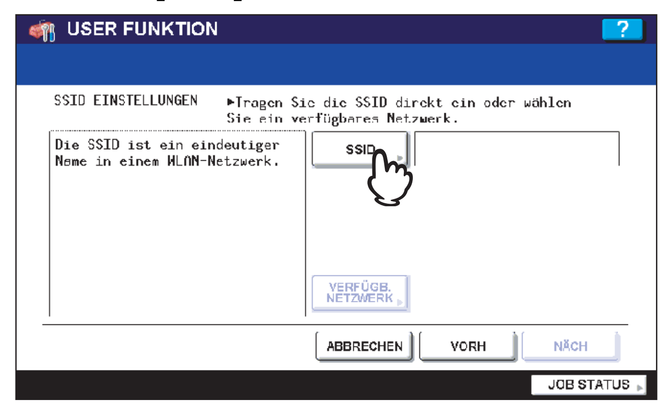
Wenn als Netzwerktyp der Ad Hoc Modus ausgewählt ist, können Sie die SSID manuell eingeben.



Wenn Sie nicht wissen, wie die SSID definiert werden muss, lesen Sie folgenden Abschnitt.
📖 S.13 “SSID definieren”

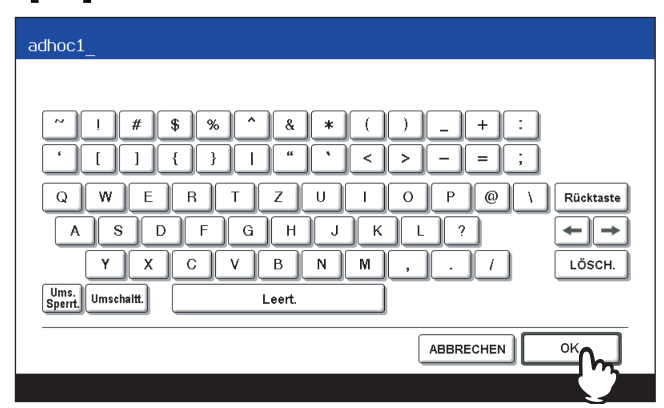
SSID manuell eingeben

1 Drücken Sie [SSID].



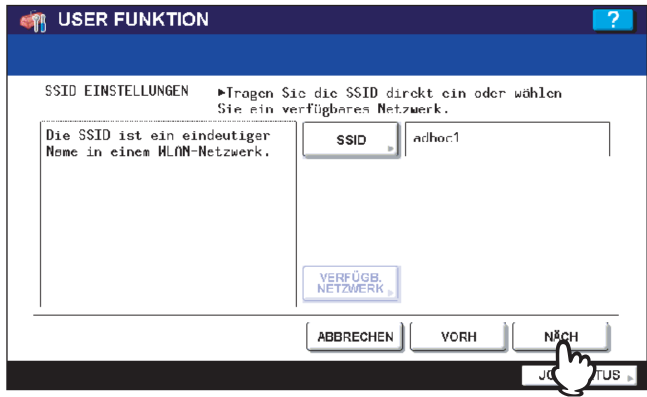
- Das Menü für die Buchstabeneingabe erscheint.

2 Geben Sie die SSID mit der angezeigten Tastatur und den Zifferntasten ein und drücken Sie [OK].

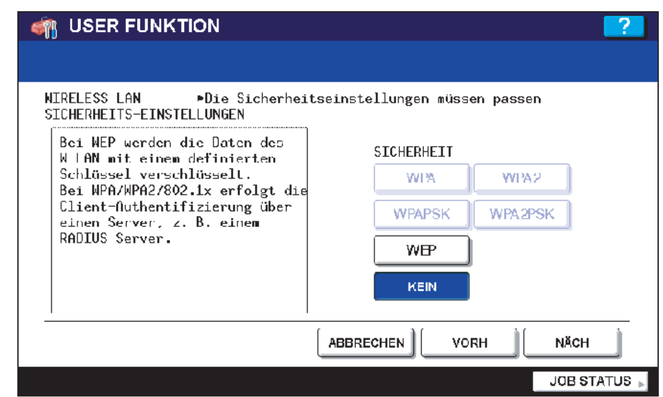


- Der Bildschirm SSID kehrt zurück.

3 Drücken Sie [NÄCH].



4 **Das Fenster WIRELESS LAN SICHERHEITS-EINSTELLUNGEN wird angezeigt.**



- Fahren Sie mit dem Definieren des Sicherheitsmodus fort.
  S.21 “Sicherheitsmodus wählen”

■ Sicherheitsmodus wählen

Wählen Sie nach der SSID einen geeigneten Sicherheitsmodus für Ihr W-LAN.
Die Vorgehensweise ist je nach Typ des Sicherheitsmodus unterschiedlich.
📖 S.32 “WEP auswählen”
📖 S.34 “Keinen Sicherheitsmodus wählen”

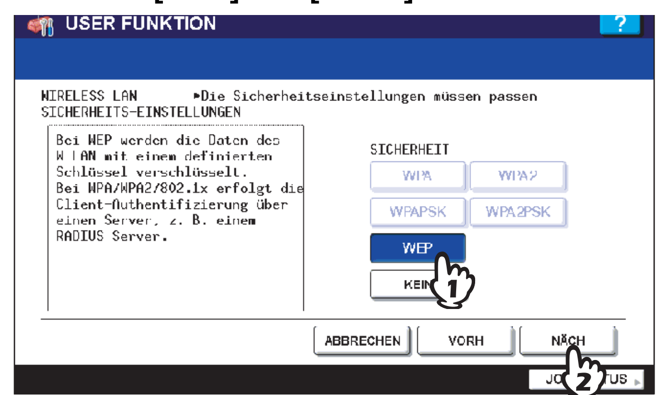
Hinweise

- Für den Ad Hoc Modus stehen nur WEP oder KEINE als Sicherheit zur Verfügung.
- Wenn Sie nicht wissen, welchen des Sicherheitsmodus Sie wählen sollen, lesen Sie folgenden Abschnitt.
  📖 S.13 “Sicherheitsmodus definieren”

WEP auswählen

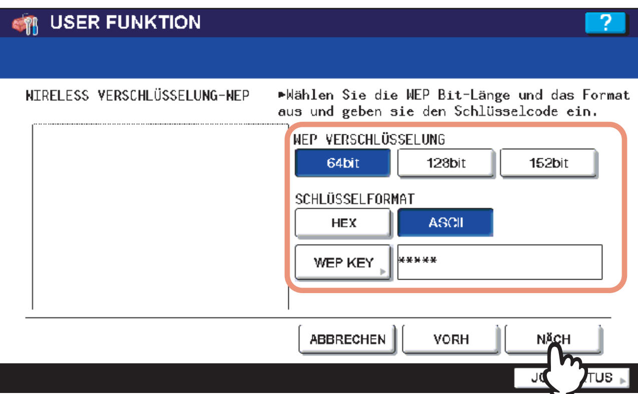
WEP ist eine Datenverschlüsselungsmethode mit WEP-Schlüssel zwischen Access Point und den anderen WLAN-Geräten.

1 Drücken Sie [WEP] und [NÄCH].



- Das Fenster VERSCHLÜSSELUNG - WEP wird angezeigt.

2 Definieren Sie folgende Positionen und drücken Sie [NÄCH].



- **WEP VERSCHLÜSSELUNG**
  Wählen Sie die Bit-Länge des WEP-Schlüssels.
- **EINGABEMETHODE SCHLÜSSEL**
  Wählen Sie den Zeichencode des WEP-Schlüssels.

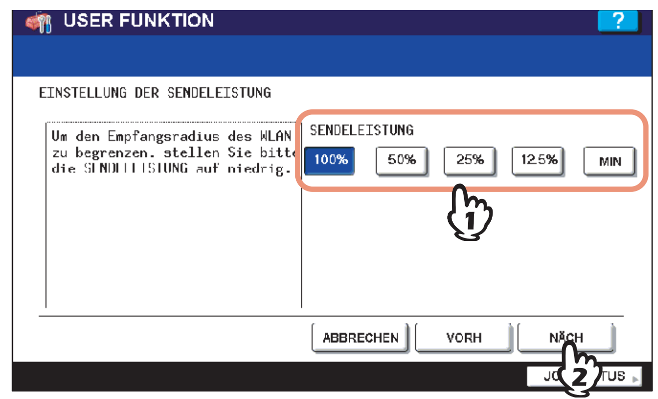
- **[WEP SCHLÜSSEL]**
  Drücken Sie darauf, um den WEP-Schlüssel einzugeben.
  Die maximale Länge des WEP-Schlüssels ist abhängig von der WEP-Verschlüsselung und der Schlüssel-Eingabemethode.

	64bit	128bit	152bit
HEX :	10	26	32
ASCII :	5	13	16

Tipp

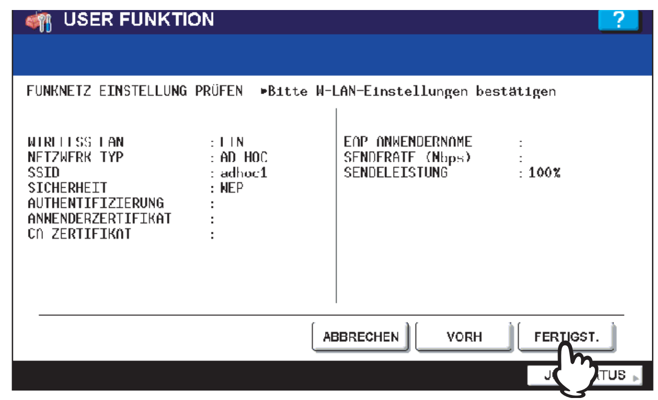
Das Eingabefenster wird angezeigt. Geben Sie den Wert über die angezeigte Tastatur und die Zifferntasten ein und drücken Sie [OK], um den Eintrag zu bestätigen.

3 Wählen Sie die Sendeleistung und drücken Sie [NÄCH].



- Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].

4 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

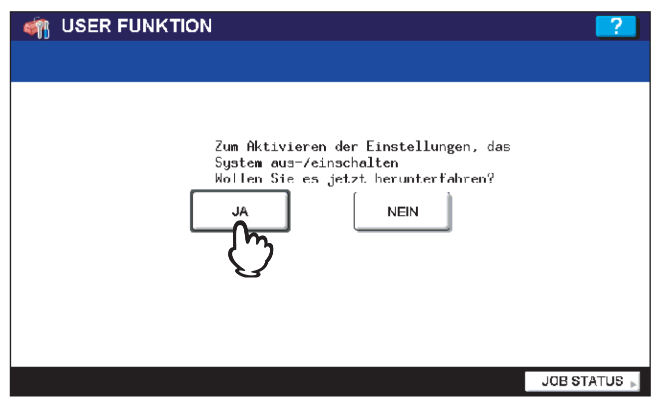


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

5 **Drücken Sie [JA], um das System herunter zu fahren.**



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

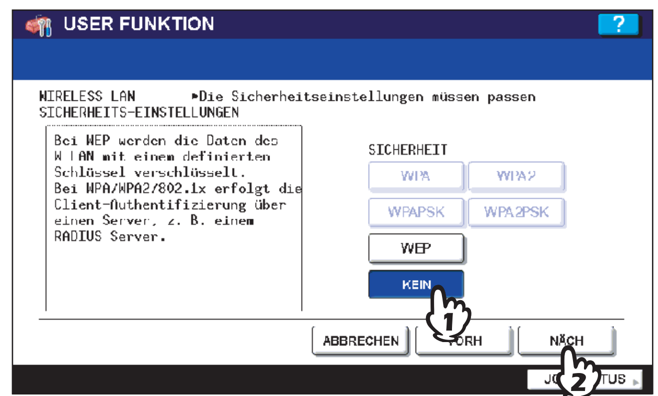
Keinen Sicherheitsmodus wählen

Sie können das W-LAN auch ungesichert betreiben.

Hinweis

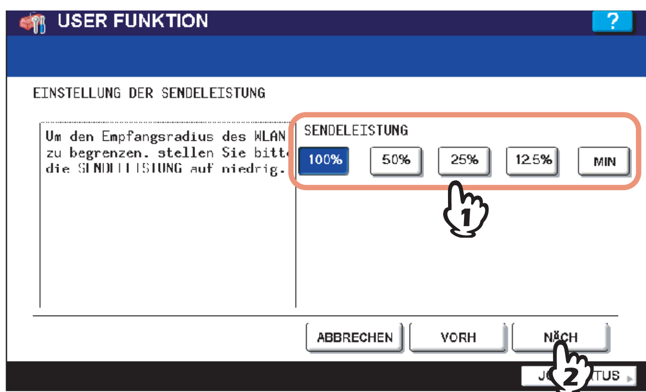
Wenn Sie dies einstellen, kann sich jeder, der die SSID in Erfahrung bringt, mit dem W-LAN verbinden. Wir empfehlen daher dringend einen Sicherheitsmodus einzustellen.

1 Drücken Sie [KEIN] und [NÄCH].



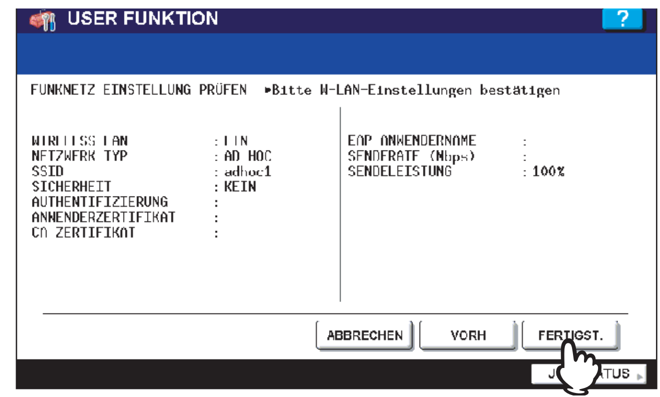
- Die Fenster SENDELEISTUNG und SENDERATE werden angezeigt.

2 Wählen Sie die Sendeleistung und drücken Sie [NÄCH].



- Wählen Sie eine niedrige Sendeleistung, wenn Sie den Empfangsbereich verkleinern wollen. Wählen Sie ansonsten [100%].

3 Prüfen Sie die Einstellungen und drücken Sie [FERTIGST.].

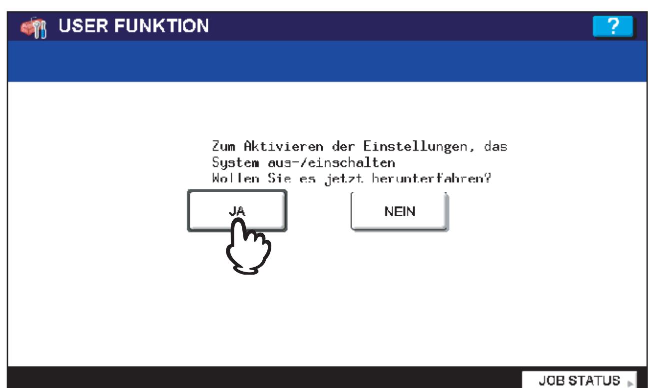


- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

Tipp

Um Einstellungen zu ändern, drücken Sie [ZURÜCK] und wiederholen die beschriebenen Bedienungsschritte.

4 Drücken Sie [JA], um das System herunter zu fahren.



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

W-LAN deaktivieren

Wenn Sie W-LAN deaktivieren, wird die interne NIC aktiviert.
Um das System über die on-board NIC an ein Netzwerk anzuschließen, müssen Sie das W-LAN deaktivieren.

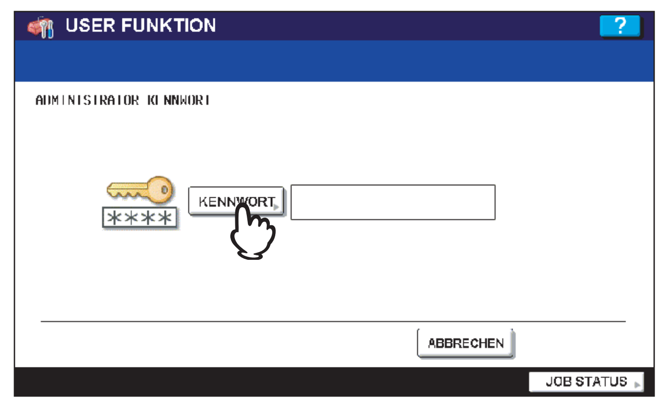
W-LAN deaktivieren

1 **Drücken Sie [USER FUNCTIONS] am Bedienfeld, um das Funktionsmenü aufzurufen.**

2 **Drücken Sie [ADMIN].**

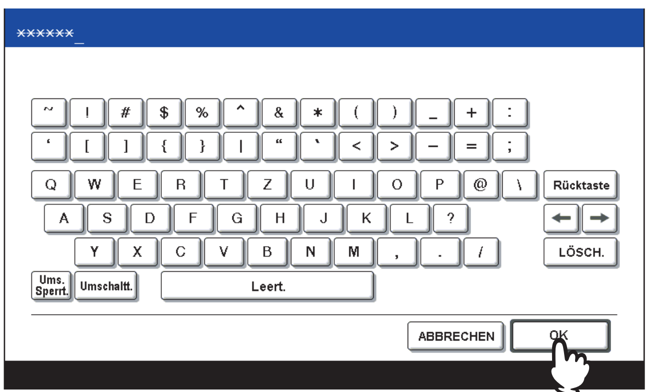
- Der Eingabebildschirm für das Administratorkennwort wird angezeigt.

3 **Drücken Sie [KENNWORT].**



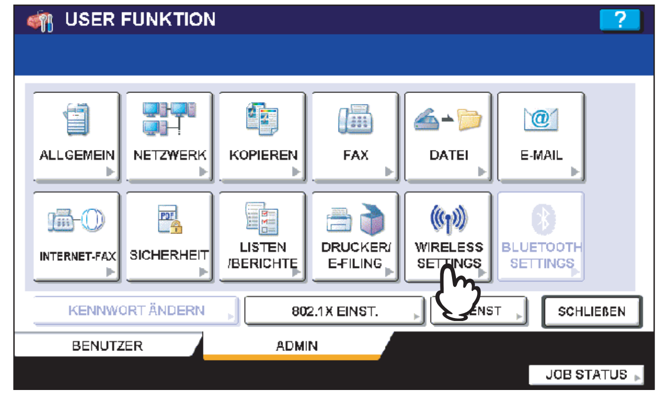
- Das Eingabefenster wird angezeigt.

4 **Geben Sie das Administratorkennwort ein und drücken Sie [OK].**



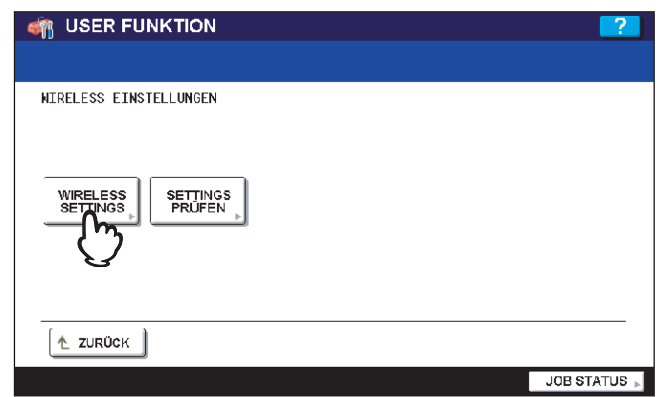
- Das Menü ADMIN wird angezeigt.

5 **Drücken Sie [WIRELESS SETTINGS].**



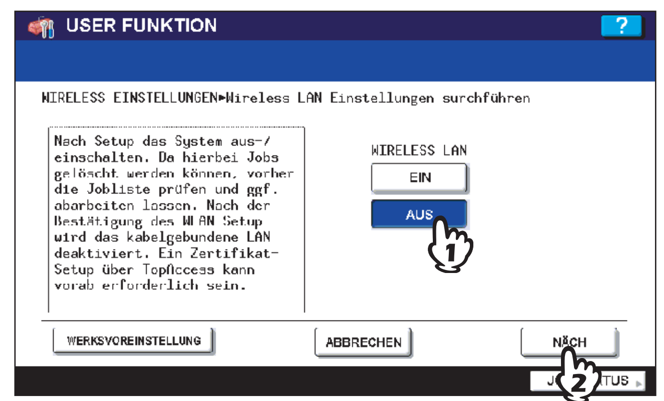
- Das WLAN-Menü wird angezeigt.

6 Drücken Sie [WIRELESS SETTINGS].



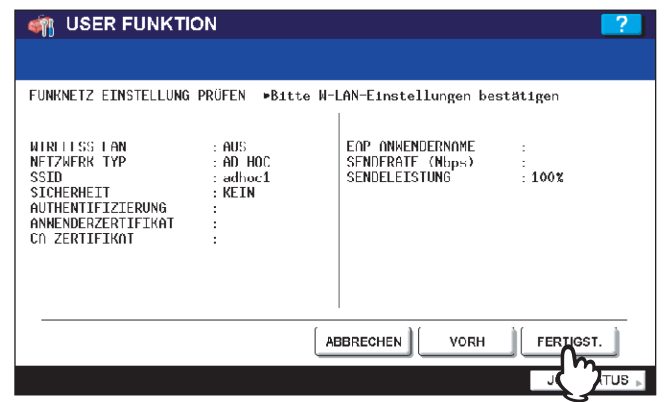
- Das Fenster WLAN wird angezeigt.

7 Drücken Sie [AUS] und [NÄCH].



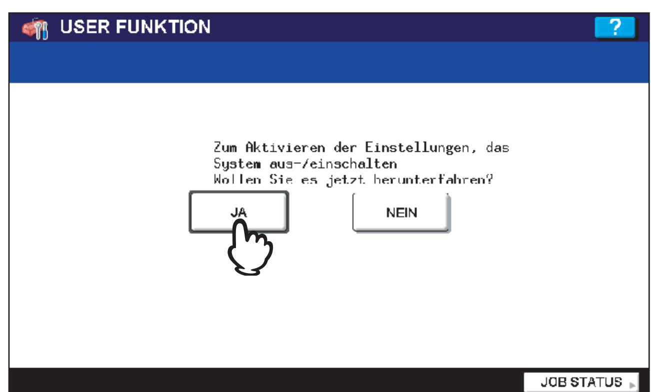
- Das Fenster NETZWERK TYP wird angezeigt.

8 Drücken Sie [FERTIGST.].



- Der Bildschirm zum Herunterfahren des Systems wird angezeigt.

9 Drücken Sie [JA], um das System herunter zu fahren.



- Die Einstellungen werden erst nach einem Neustart des Gerätes wirksam.

2

ANHANG

In diesem Abschnitt finden Sie die Spezifikationen und ein Glossar.

Spezifikationen

Position	Beschreibung
Sendeformat	IEEE 1802.11g Standard Spreizspektrummodulation(DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
Sendegeschwindigkeit	54, 24, 11, 5.5, 2, 1Mbps (fest/automatisch)
Zugriffsmethode	CSMA/CA
Sendepaket	IEEE 802.11g frame
Kategorie	Datenübertragungssystem mit geringer Leistungsabgabe (2400 bis 2472MHz)
Leistungsabgabe	max. 10mW/MHz
Sicherheit	Statisches WEP Schlüssellänge: 64bit, 128bit, 152bit WPA/WPA2: PSK (TKIP, AES(CCMP)) WPA/WPA2: TLS/PEAP (TKIP, AES(CCMP)) *1 Unterstützte RADIUS-Server Funk Odyssey Server (WiFi Standard) Microsoft Windows Server 2000/2003/2008 *2 Unterstützte RADIUS-Server Microsoft Windows Server 2000/2003/2008
Modi	Infrastruktur Modus, Ad Hoc Modus
W-LAN Ein/Aus	verfügbar
LAN/W-LAN gleichzeitig	nicht verfügbar
W-LAN/Bluetooth gleichzeitig	verfügbar

Fehlerbehebung

Fehlermeldungen

Zu den W-LAN Fehlermeldungen siehe nachfolgende Tabelle.

Fehlermeldung	Fehlerbehebung
Bad certificate	Ein nicht unterstütztes Zertifikat ist installiert. Installieren Sie das entsprechende Zertifikat neu. Unterstützt werden nur md5RSA- und sha1RSA-Zertifikate.
Bad record mac	Fehler bei SSL-Schlüsseltausch. Schalten Sie das System aus und wieder ein.
Certificate expired	Das Zertifikat ist abgelaufen. Prüfen Sie die Zeiteinstellung und ob das Zertifikat abgelaufen ist.
Certificate revoke	Das Zertifikat wurde abgewiesen. Fragen Sie Ihren Administrator.
Certificate unknown	Das installierte CA-Zertifikat kann nicht als Server-Zertifikat fungieren. Achten Sie auf richtige Installation der Zertifikate.
Decompression failure	Das Gerät unterstützt nicht die SSL-Komprimierung. Deaktivieren Sie die SSL-Komprimierung auf dem RADIUS-Server.
Handshake failure	Eine nicht unterstützte Verschlüsselung ist eingestellt. Achten Sie auf die korrekte Verschlüsselungsmethode.
Illegal parameter	Eine nicht unterstützte Version des TLS-Protokolls wird verwendet. Achten Sie auf die richtige Version des TLS-Protokolls.
No certificate	Es ist kein Zertifikat installiert oder der Zertifikat-Name wurde nicht ausgewählt. Achten Sie auf korrekte Installation vom Zertifikat und geben Sie den Zertifikat-Namen korrekt ein.
Peer error certificate	Das installierte CA-Zertifikat kann für die Prüfung des Server-Zertifikates im RADIUS-Server nicht verwendet werden.. Achten Sie auf korrekte Installation des CA-Zertifikats.
Peer error no certificate	Der RADIUS-Server versucht eine Kommunikation mit dem Zertifikat über das TLS-Protokoll.
Peer no cipher	Der RADIUS-Server verlangt eine vom Gerät nicht unterstützte Verschlüsselung.
Peer error unsupported certificate type	Das Gerät verwendet ein Zertifikat, das der RADIUS-Server nicht unterstützt.
Peer unexpected message	Der RADIUS-Server sendet eine Nachricht, die nicht dem TLS-Standard entspricht. Prüfen Sie die Einstellungen auf dem RADIUS-Server.
Unknown remote error type	Der RADIUS-Server sendet eine Warnmeldung über ein illegales TLS.
Unsupported certificate	Das Gerät verwendet ein Zertifikat, das der RADIUS-Server nicht unterstützt.
Unknown ca	Das installierte CA-Zertifikat kann nicht für die Prüfung der Server-Zertifikats auf dem RADIUS-Server verwendet werden. Achten Sie auf die Installation eines korrekten CA-Zertifikats.
Unable to connect	Wenden Sie sich an Ihren Administrator.

Keine Verbindung zum TOSHIBA Multifunktionssystem möglich

Bitte prüfen Sie in diesem Fall folgende Punkte.
- Das Anwenderzertifikat ist nicht abgelaufen.
- Die Einstellungen von Access Point und Netzwerk sind korrekt.

Glossar

Ad Hoc
Die einzelnen WLAN-Geräte kommunizieren direkt untereinander ohne Access Point.

AP (Access Point)
Eine Basisstation, über die alle WLAN-Geräte kommunizieren und die besonders für große WLAN-Netzwerke geeignet ist.

Bridge
Ein Gerät, um zwischen LANs zu vermitteln. Die Bridge bestimmt anhand der Adressen, ob Daten an bestimmte Netzknoten gesendet werden. Es kann zur Verbindung zweier Netzwerke mit unterschiedlichen Protokollen oder für eine Rundsendung an alle Computer für alle Netzwerke verwendet werden.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
Dies ist eine Methode zur Kollisionsvermeidung bei Übertragungsvorgängen. Die WLAN-Geräte horchen vor dem Senden, ob bereits eine Sendung anderer WLAN-Geräte durchgeführt wird. CSMA/CA ist CSMA mit zusätzlicher Kollisionsvermeidungs-Funktion.

DS (Direct Sequence)
Ein spektral verteiltes Signal, das in einem engen Frequenzband durch Phasenmodulation der Trägerfrequenz breitbandig gespreizt wird.

ESS ID (Extended Service Set ID)
Die ESS ID wird ähnlich einem Namen einem WLAN zugewiesen, zu dem die jeweilige Einheit gehört. Zwischen WLAN-Geräten mit unterschiedlichen Namen ist keine Kommunikation möglich.
Ein WLAN kann jedoch durch unterschiedliche ESS IDs aufgeteilt werden.

IEEE (Institute of Electrical Electronics Engineers)
Eine Organisation zur Standardisierung und Normenbildung.
Committee 802 ist zuständig für LAN-bezogene Angelegenheiten.

IEEE 802.11b/IEEE 802.11g
Der WLAN-Standard von der IEEE.

Infrastruktur
Ein System zur Integration kabelloser Netzwerke mit kabelgebundenen Netzwerken.

Kanal
Ist gleichbedeutend mit einem Fernseh- oder Radiokanal. Der IEE 802.11 Standard verwendet das 2,4 Bit 2,472 Gigahertz ISM-Band und teilt dieses in 11 Kanäle auf. Alle WLAN-Geräte können nur über den gleichen Kanal miteinander kommunizieren.

LAN (Local Area Network)
Ein Netzwerk innerhalb eines begrenzten Bereichs.
Auch Intranet genannt.

Roaming
Der Begriff kommt aus dem Mobilfunkbereich und bezeichnet ein Übergabeverfahren zwischen den Funkzellen, damit auch bei Bewegung eine unterbrechungsfreie Kommunikation möglich ist. Für das WLAN ist der AP (die Basisstation) die Funkzelle und der PC (Anwender) entspricht dem Telefonteilnehmer.

Router
Ein Gerät zur Vermittlung zwischen LANs. Der Router ermittelt die Datenadresse aus Netzwerkadresse und einzelner Computeradresse. Wird besonders in großen LAN-Systemen eingesetzt, um den Verkehr über die Kommunikationsleitungen zu reduzieren.

RSSI (Receive Signal Strength Indication)
Eine numerische Anzeige der eingehenden Signalstärke.

RTS (Request To Send)
Bei der Kommunikation über den AP werden Sendungen über CSMA/CA + RTS kontrolliert. Bei RTS fragt das WLAN-Gerät den AP, ob er sendebereit ist und sendet nur nach einem OK. Dies verhindert unerwünschte Kollisionen.

Spectrum Diffusion Transmission

Bei dieser Methode werden Signale, die normalerweise über ein gegebenes, begrenztes Frequenzband laufen, in einem engen Frequenzbereich moduliert (primäre Modulation), danach für ein weites Frequenzspektrum moduliert (zweite Modulation), um die Bandbreite zu erhöhen.

INDEX

MULTIFUNKTIONALE DIGITALE SYSTEME WIRELESS LAN MODUL
Bedienungsanleitung für Wireless LAN

GN-1050

TOSHIBA TEC CORPORATION
2-17-2, HIGASHIGOTANDA, SHINAGAWA-KU, TOKYO, 141-8664, JAPAN

Ver00 2008-05